JOURNAL OF ALGEBRA 38, 414–452 (1976)

Hopf Algebra Orders Determined by Group Valuations*

RICHARD GUSTAVUS LARSON

Department of Mathematics, University of Illinois at Chicago Circle, Chicago, Illinois 60680

Communicated by D. Buchsbaum

Received August 29, 1974

Hopf algebra orders in the group algebra of a finite group can be used to get information on the representation theory of the group. In this paper, we describe a class of such orders that arises from group valuations on the group and use properties of these orders to get a new bound on the degrees of the absolutely irreducible representations of the group.

In Section 1, we discuss the basic properties of group valuations. A group valuation is a real-valued function on the group that satisfies conditions that reflect the product and commutator relations on the group. We also introduce weighted filtrations. These correspond to group valuations and are sometimes more convenient for computation. Next, Hopf algebra orders are introduced and in Section 3, their relation to group valuations is discussed. There is a one–one correspondence between group valuations satisfying certain conditions reflecting the orders of the group elements and the pth power map (the p-adic order-bounded group valuations) and certain Hopf algebra orders in the group algebra. An important invariant associated with a Hopf algebra order A is $\epsilon(L_A)$, where L_A is the ideal of left integrals in A. In Section 4, we compute $\epsilon(L_A)$ for those Hopf algebra orders associated with p-adic order-bounded group valuations. In Section 5, we apply the results of Section 4 to get a new bound on the degrees of the absolutely irreducible representations of a finite group. In Section 6, we compare the bound given in Section 5 with the bound given in Ito's theorem (the degree of an absolutely irreducible representation must divide the index of any normal abelian subgroup) for the groups of order 2^n, $0 \leqslant n \leqslant 6$. The work in the first six sections is all local; in Section 7, we briefly describe the global situation, and discuss some of the open questions involving Hopf algebra orders.

In this paper, we assume that the reader is familiar with the results and techniques of [8]. Throughout this paper, k is an algebraic number field and

* Research partially supported by NSF Grant GP 28420 and by a sabbatical from the University of Illinois at Chicago Circle.

R is the ring of integers in k. By a valuation on k, we mean an exponential nonarchimedean valuation.

1. Group Valuations and Weighted Filtrations

In this section, we define group valuations, order bounded group valuations, and p-adic order-bounded group valuations. Group valuations were first discussed by Zassenhaus in [20]. The group valuations used in this paper are less general than his: We consider only order-bounded group valuations. For these valuations, our definition of p-adicity is equivalent to his. After proving some basic results about order-bounded group valuations, we define a weighted filtration on a finite group and discuss the relation between order-bounded group valuations and weighted filtrations. In later sections, we sometimes find it more convenient to use the associated weighted filtration when doing computations involving a group valuation.

Definition 1.1. Let G be a finite group. A *group valuation* is a function $\xi\colon G \to \mathbf{R} \cup \{\infty\}$ satisfying

(1) $\xi(g) \geqslant 0$; $\xi(g) = \infty$, if and only if $g = 1$.

(2) $\xi(gh) \geqslant \min\{\xi(g), \xi(h)\}$.

(3) $\xi([g, h]) \geqslant \xi(g) + \xi(h)$.

Let ν be a fixed valuation on k. If the range of ξ is contained in the range of ν and if

$$\begin{aligned} \xi(g) &= 0, && \text{if order}(g) \text{ is not a prime power,} \\ &\leqslant \nu(q)/\varphi(\text{order}(g)), && \text{if order}(g) = q^s \text{ is a prime power,} \end{aligned}$$

where φ is the Euler totient function, then ξ is said to be *order bounded* (*with respect to* ν). The order-bounded group valuation ξ is said to be *p-adic* if

$$\xi(g^p) \geqslant p\xi(g)$$

for all g in G.

It is clear that if H is a subgroup of G and ξ is a group valuation on G, then $\xi \mid H$ is a group valuation on H. If ξ is order bounded, so is $\xi \mid H$. If ξ is p-adic, so is $\xi \mid H$. The situation for quotient groups is more complicated and will be discussed (in terms of weighted filtrations) at the end of this section.

Let ξ be a group valuation on G. For each $x \in \mathbf{R}$, define

$$G_x = \{g \in G \mid \xi(g) \geqslant x\}.$$

From Definition 1.1(2) it follows that G_x is a subgroup of G. From Definition 1.1(3) it follows that $[G_x, G_y] \subseteq G_{x+y}$. It is clear that if $x \leqslant y$, then $G_x \supseteq G_y$, that $\bigcap G_x = \{1\}$, and that $G = G_0$.

PROPOSITION 1.2. *There is a one-one correspondence between group valuations on G and order reversing functions $x \mapsto G_x$ from $\mathbf{R}$ to the lattice of subgroups of G satisfying*

$$\bigcap G_x = \{1\}, \qquad G_0 = G,$$

and

$$[G_x, G_y] \subseteq G_{x+y}.$$

Proof. We have shown above how the function $x \mapsto G_x$ arises from the group valuation ξ. Conversely, suppose that $x \mapsto G_x$ is such a function. Define

$$\begin{aligned} \xi(g) &= \sup\{x \mid g \in G_x\}, \qquad \text{if} \quad g \neq 1, \\ &= \infty, \qquad \text{if} \quad g = 1. \end{aligned}$$

It is immediate that $\xi(g) \geqslant 0$, and $\xi(g) = \infty$ if and only if $g = 1$. The fact that the G_x are subgroups implies that $\xi(gh) \geqslant \min\{\xi(g), \xi(h)\}$. The fact that $[G_x, G_y] \subseteq G_{x+y}$ implies that $\xi([g, h]) \geqslant \xi(g) + \xi(h)$. Therefore, ξ is a group valuation. It is clear that the maps from valuations to functions on $\mathbf{R}$ and from functions on $\mathbf{R}$ to valuations are inverse to each other. We thus have a one-one correspondence between group valuations and functions $x \mapsto G_x$ as described.

COROLLARY 1.3. *Let ξ be a group valuation on G. Then,*

$$\xi(g) = \xi(g^{-1}), \qquad \textit{for all } g \textit{ in } G$$

and

$$\xi(ghg^{-1}) = \xi(h), \qquad \textit{for all } g, h \textit{ in } G.$$

If H is the normal subgroup generated by a set A satisfying $\xi(a) \geqslant r$ for all a in A, then $\xi(h) \geqslant r$ for all h in H.

Proof. The first assertion follows from the fact that G_x is a subgroup; the second assertion follows from the fact that G_x is normal in G, which in turn follows from the fact that $[G, G_x] = [G_0, G_x] \subseteq G_x$. The third assertion follows from the fact that $\xi(a) \geqslant r$ implies $A \subseteq G_r$, which implies that $H \subseteq G_r$.

Let $G_+ = \bigcup_{x>0} G_x$. The following Lemma is immediate.

LEMMA 1.4. *G_+ is a normal nilpotent subgroup of G.*

We partially order the set of real-valued functions on G in the usual manner: $f_1 \leqslant f_2$ if $f_1(g) \leqslant f_2(g)$ for all g in G.

LEMMA 1.5. *Let $\{\xi_i\}$ be a totally ordered set of order-bounded group valuations and let ξ be defined by*

$$\xi(g) = \sup\{\xi_i(g)\}.$$

Then, ξ is an order-bounded group valuation. If each ξ_i is p-adic, then ξ is p-adic.

Proof. It is clear that $\xi(g) \geqslant 0$. The fact that the ξ_i are order bounded implies that $\xi(g) < \infty$ for $g \neq 1$. If $\xi(gh) < \min\{\xi(g), \xi(h)\}$, then $\xi(gh) < \xi(g)$ and $\xi(gh) < \xi(h)$. Therefore, for some i,

$$\xi_i(gh) \leqslant \xi(gh) < \xi_i(g) \leqslant \xi(g)$$

and

$$\xi_i(gh) \leqslant \xi(gh) < \xi_i(h) \leqslant \xi(h),$$

so $\xi_i(gh) < \min\{\xi_i(g), \xi_i(h)\}$, which is impossible. If $\xi([g, h]) < \xi(g) + \xi(h)$, let $\epsilon = \xi(g) + \xi(h) - \xi([g, h])$. For some i,

$$\xi(g) - \epsilon/2 < \xi_i(g) \leqslant \xi(g)$$

and

$$\xi(h) - \epsilon/2 < \xi_i(h) \leqslant \xi(h).$$

Adding these two pairs of inequalities, we get

$$\xi(g) + \xi(h) - \epsilon < \xi_i(g) + \xi_i(h) \leqslant \xi(g) + \xi(h),$$

so

$$\xi([g, h]) < \xi_i(g) + \xi_i(h) \leqslant \xi_i([g, h]),$$

which is impossible. Note that in the above, we used the fact that the family $\{\xi_i\}$ was totally ordered to simultaneously satisfy the inequalities. It is immediate that ξ is order bounded.

Suppose that each ξ_i is p-adic. If $\xi(g^p) < p\xi(g)$, then, for some i, $\xi(g^p) < p\xi_i(g) \leqslant p\xi(g)$, so $\xi_i(g^p) \leqslant \xi(g^p) < p\xi_i(g)$, which is impossible. This completes the proof of the Lemma.

Applying Lemma 1.5 and Zorn's lemma we get:

PROPOSITION 1.6. *Let G be a finite group. There exist maximal order-bounded group valuations on G. There exist maximal p-adic order-bounded group valuations on G.*

The proof of the following proposition will be given in Section 3.

PROPOSITION 1.7. *Let G be a finite group. Every maximal order-bounded group valuation on G is p-adic.*

It is often desirable to find maximal order-bounded group valuations whose existence is asserted in Proposition 1.6. The following algorithm is helpful in finding them in certain cases. We denote $G - \{1\}$ by G^*.

ALGORITHM 1.8. *Let G be a finite group, and let f be a real-valued function on G^*. Fix an enumeration $g_0 = 1, g_1, \ldots, g_{n-1}$ of G. Define*

$$\xi_0'(g) = \xi_0(g) = f(g), \qquad \textit{for} \quad g \neq 1,$$
$$\xi_0'(1) = \xi_0(1) = \infty.$$

Set $i = 1$.

Step 1. *For each $j = 0, \ldots, n-1$, set*

$$\xi_i(g_j) = \max\{\xi_{i-1}(g_j), \min\{\xi_{i-1}(g_r), \xi_{i-1}(g_s)\}, \xi_{i-1}(g_t) + \xi_{i-1}(g_u)\},$$
$$\xi_i'(g_j) = \max\{\xi_{i-1}'(g_j), \min\{\xi_{i-1}'(g_r), \xi_{i-1}'(g_s)\}, \xi_{i-1}'(g_t) + \xi_{i-1}'(g_u), p\xi_{i-1}'(g_v)\},$$

where (r, s) ranges over all pairs such that $g_j = g_r g_s$, (t, u) ranges over all pairs such that $g_j = [g_t, g_u]$, and v ranges over all indices such that $g_j = g_v{}^p$. If

$$\xi_i(g_j) > \nu(p)/\varphi(\mathrm{order}(g_j)),$$

or

$$\xi_i'(g_j) > \nu(p)/\varphi(\mathrm{order}(g_j)),$$

for some j, the algorithm fails.

Step 2. *If for each $j = 0, \ldots, n-1$, $\xi_i(g_j) = \xi_{i-1}(g_j)$ and $\zeta_i'(g_j) = \xi_{i-1}'(g_j)$, set $\xi = \xi_i$ and $\xi' = \xi_i'$; the algorithm terminates successfully. Otherwise, set $i = i + 1$ and return to Step* 1.

PROPOSITION 1.9. *Let G be a finite group, and let f be a nonnegative real-valued function on G^*. If there exists an order-bounded group valuation $\zeta \geqslant f$, after a finite number of steps, Algorithm* 1.8 *terminates successfully with $\zeta \geqslant \xi$. If ζ is p-adic, $\zeta \geqslant \xi'$ also. In this case ξ is the smallest order-bounded group valuation $\geqslant f$, and ξ' is the smallest p-adic order-bounded group valuation $\geqslant f$. If there exists no order-bounded group valuation $\geqslant f$, after a finite number of steps, Algorithm* 1.8 *fails.*

Proof. We first show that for any function f, Algorithm 1.8 either terminates successfully, or fails after a finite number of steps. Let C be the set of all sums of elements of $\mathrm{Im} f$, and let $D_j = C \cap [0, \nu(p)/\varphi(\mathrm{order}(g_j))]$. Since $\mathrm{Im} f$ is finite and contains only nonnegative numbers, it follows that D_j is finite. Suppose that Algorithm 1.8 does not fail at any point. For each j, we have nondecreasing sequences

$$\xi_0(g_j) \leqslant \xi_1(g_j) \leqslant \cdots \leqslant \xi_i(g_j) \leqslant \cdots$$

and

$$\xi_0'(g_j) \leqslant \xi_1'(g_j) \leqslant \cdots \leqslant \xi_i'(g_j) \leqslant \cdots.$$

Since all the terms in these sequences lie in the finite set D_j, the sequences must stabilize at some point i. Do this for $j = 0,..., n-1$ and take the largest i that occurs. Then, Algorithm 1.8 terminates successfully at stage $i+1$.

Examining the definition of the algorithm, we see that if the algorithm terminates successfully at stage i, then ξ_i is an order-bounded group valuation $\geqslant f$, and ξ_i' is a p-adic order bounded group valuation $\geqslant f$. The last assertion of the proposition follows from these facts.

We now show by induction on i that if $\zeta \geqslant f$ is an order-bounded group valuation, then $\zeta \geqslant \xi_i$ for all i. This assertion is clear for $i = 0$. Suppose that it holds for $i - 1$. Then,

$$\begin{aligned}
&\zeta(g_j) \geqslant \xi_{i-1}(g_j),\\
&\zeta(g_j) \geqslant \min\{\zeta(g_r), \zeta(g_s)\} \geqslant \min\{\xi_{i-1}(g_r), \xi_{i-1}(g_s)\},\\
&\zeta(g_j) \geqslant \zeta(g_t) + \zeta(g_u) \geqslant \xi_{i-1}(g_t) + \xi_{i-1}(g_u).
\end{aligned}$$

Since $\xi_i(g_j)$ is the maximum of the right-hand sides of these inequalities, $\zeta(g_j) \geqslant \xi_i(g_j)$. A similar argument shows that if ζ is p-adic, then $\zeta \geqslant \xi_i'$ for all i.

Suppose now that there exists an order-bounded group valuation $\zeta \geqslant f$. Let $\zeta' \geqslant \zeta$ be a maximal order-bounded group valuation. By Proposition 1.7 ζ' is p-adic. Therefore,

$$\nu(p)/\varphi(\mathrm{order}(g_j)) \geqslant \zeta'(g_j) \geqslant \xi_i(g_j),\ \xi_i'(g_j)$$

for all i, j. Therefore, the algorithm cannot fail. Therefore, it must terminate successfully. This completes the proof of the Proposition.

Algorithm 1.8 is a reasonably practical way of finding order-bounded group valuations: it was programmed on a PDP-10 computer and was used extensively to produce examples of group valuations in the early stages of this research.

We can think of a group valuation ξ as a point (x_j) in real $(n-1)$-dimensional space, where $x_j = \xi(g_j)$. The set of all valuations then can be described as the set of solutions of the system of inequalities

$$\begin{aligned}
&x_j \geqslant 0,\\
&x_j \geqslant \min\{x_r, x_s\},\\
&x_j \geqslant x_t + x_u,\\
&x_j \leqslant \nu(p)/\varphi(\mathrm{order}(g_j)),
\end{aligned}$$

and for p-adic valuations,

$$x_j \geqslant px_v .$$

Because the second inequality is not linear, the set of solutions will not be convex in general. It is sometimes desirable to have an alternate description of group valuations that does not explicitly use nonlinear conditions.

We now give a characterization of order-bounded group valuations in terms of functions on series of normal subgroups. We will use this characterization in Sections 3 and 4. Let ν be a fixed valuation, and let p be the rational prime for which $\nu(p) \neq 0$.

DEFINITION 1.10. Let G be a finite group. A *filtration base in G* is a set $\mathscr{B}$ of normal subgroups, all of whose orders are powers of p, which is totally ordered by inclusion. A *weighted filtration in G* is a pair $(\mathscr{B}, \rho)$ where $\mathscr{B}$ is a filtration base and ρ is a function from $\mathscr{B}$ to $\mathbf{R} \cup \{\infty\}$ satisfying

(1) If $M \supset N$, then $\rho(M) \leqslant \rho(N)$.

(2) $\rho(M) > 0$; $\rho(M) = \infty$ if and only if $M = \{1\}$.

(3) If P is the smallest group in $\mathscr{B}$ containing $\{[m, n] \mid m \in M, n \in N\}$, then $\rho(P) \geqslant \rho(M) + \rho(N)$.

(4) $\rho(M) \leqslant \min\{\nu(p)/\varphi(\text{order}(m)) \mid m \in M\}$, for all $M \in \mathscr{B}$.

The weighted filtration $(\mathscr{B}, \rho)$ is called *strict* if $M \supset N$ implies $\rho(M) < \rho(N)$. It is called *p-adic* if $\rho(N) \geqslant p\rho(M)$, where N is the smallest group in $\mathscr{B}$ containing $\{m^p \mid m \in M\}$. It is called *complete* if the groups in $\mathscr{B}$ form a composition series for the largest group in $\mathscr{B}$.

A weighted filtration $(\mathscr{B}', \rho')$ is said to be an *extension* of the weighted filtration $(\mathscr{B}, \rho)$ if $\mathscr{B}' \supseteq \mathscr{B}$ and $\rho' \mid \mathscr{B} = \rho$. The extension is called *trivial* if

$$\rho'(N) = \max\{\rho(M) \mid M \supseteq N, M \in \mathscr{B}\},$$

for all $N \in \mathscr{B}'$.

LEMMA 1.11. *Let $(\mathscr{B}, \rho)$ be a weighted filtration. Then, there exists a complete weighted filtration $(\mathscr{B}', \rho')$ that is a trivial extension of $(\mathscr{B}, \rho)$. If $(\mathscr{B}, \rho)$ is p-adic, then $(\mathscr{B}', \rho')$ is p-adic.*

Proof. Let $\mathscr{B}'$ be a composition series of the largest group in $\mathscr{B}$ that refines the series $\mathscr{B}$. Define ρ' by

$$\rho'(N) = \max\{\rho(M) \mid M \supseteq N, M \in \mathscr{B}\}.$$

It is immediate $\rho' \mid \mathscr{B} = \rho$, that $\rho(M) \leqslant \rho(N)$ if $M \supset N$, that $\rho(M) > 0$, and that $\rho(M) = \infty$ if and only if $M = \{1\}$.

Let $M, N \in \mathscr{B}'$, and let P be the smallest group in $\mathscr{B}'$ containing $\{[m, n] \mid m \in M, n \in N\}$. Let M_1 be the smallest group in $\mathscr{B}$ containing M, let N_1 be the smallest group in $\mathscr{B}$ containing N, and let Q be the smallest group in $\mathscr{B}$ containing $\{[m, n] \mid m \in M_1, n \in N_1\}$. Then, $Q \supseteq P$, so $\rho(Q) \leqslant \rho'(P)$. Therefore,

$$\rho'(P) \geqslant \rho(Q) \geqslant \rho(M_1) + \rho(N_1) = \rho'(M) + \rho'(N).$$

Also,

$$\begin{aligned}\rho'(M) &= \rho(M_1)\\ &\leqslant \min\{\nu(p)/\varphi(\text{order}(m)) \mid m \in M_1\}\\ &\leqslant \min\{\nu(p)/\varphi(\text{order}(m)) \mid m \in M\}.\end{aligned}$$

This proves that $(\mathscr{B}', \rho')$ is a complete weighted filtration extending $(\mathscr{B}, \rho)$. Suppose now that $(\mathscr{B}, \rho)$ is p-adic. Let $M \in \mathscr{B}'$ and let N be the smallest group in $\mathscr{B}'$ containing $\{m^p \mid m \in M\}$. Let M_1 be the smallest group in $\mathscr{B}$ containing M and let P be the smallest group in $\mathscr{B}$ containing $\{m^p \mid m \in M_1\}$. Then, $P \supseteq N$, so

$$\rho'(N) \geqslant \rho(P) \geqslant p\rho(M_1) = p\rho'(M).$$

Therefore, $(\mathscr{B}', \rho')$ is p-adic if $(\mathscr{B}, \rho)$ is p-adic. This completes the proof of the lemma.

We now describe a correspondence between group valuations and strict weighted filtrations. Let ξ be an order-bounded group valuation on G. Recall that $G_x = \{g \in G \mid \xi(g) \geqslant x\}$. The set $\{G_x \mid x > 0\}$ is a set of normal subgroups, each of order a power of p, which is totally ordered by inclusion. Define the function $\rho: \mathscr{B} \to \mathbf{R} \cup \{\infty\}$ by

$$\rho(M) = \min\{\xi(m) \mid m \in M\}.$$

It is immediate that ρ is strictly order-reversing, that $\rho(M) > 0$, and that $\rho(M) = \infty$ if and only if $M = \{1\}$. Let M, N be in $\mathscr{B}$ and let P be the smallest group in $\mathscr{B}$ containing $\{[m, n] \mid m \in M, n \in N\}$. Since

$$\xi([m, n]) \geqslant \xi(m) + \xi(n),$$

it follows that

$$\xi([m, n]) \geqslant \rho(M) + \rho(N).$$

Let $y = \rho(M) + \rho(N)$. We have shown that $[m, n] \in G_y$. Therefore, $P \subseteq G_y$, so $\rho(P) \geqslant \rho(G_y) \geqslant y$. This proves that $\rho(P) \geqslant \rho(M) + \rho(N)$. Since ξ is order bounded,

$$\xi(m) \leqslant \nu(p)/\varphi(\text{order}(m)).$$

Taking the minimum of both sides, we get that

$$\rho(M) \leqslant \min\{\nu(p)/\varphi(\text{order}(m)) \mid m \in M\}.$$

This proves that $(\mathscr{B}, \rho)$ is a strict weighted filtration. If ξ is p-adic, let M be in $\mathscr{B}$ and let N be the smallest group in $\mathscr{B}$ containing $\{m^p \mid m \in M\}$. Since

$$\xi(m^p) \geqslant p\xi(m),$$

it follows that

$$\xi(m^p) \geqslant p\rho(M).$$

Let $y = p\rho(M)$. We have shown that $m^p \in G_y$. Therefore, $N \subseteq G_y$, so $\rho(N) \geqslant \rho(G_y) \geqslant y = p\rho(M)$. This proves that $(\mathscr{B}, \rho)$ is p-adic, if ξ is p-adic.

Denote the strict weighted filtration constructed from ξ by $\mathbf{F}(\xi)$.

Let $(\mathscr{B}, \rho)$ be a weighted filtration. If $G \notin \mathscr{B}$, extend ρ to $\mathscr{B} \cup \{G\}$ by setting $\rho(G) = 0$. Define the function $\xi\colon G \to \mathbf{R} \cup \{\infty\}$ by

$$\xi(g) = \max\{\rho(N) \mid g \in N\}.$$

Note that $\xi(g) = \rho(N)$ for N the smallest group in $\mathscr{B} \cup \{G\}$ containing g. It is immediate that $\xi(g) \geqslant 0$ and that $\xi(g) = \infty$ if and only if $g = 1$. If $g, h \in G$, let M be the smallest group in $\mathscr{B} \cup \{G\}$ containing both g and h. Then, $gh \in M$ so

$$\xi(gh) \geqslant \rho(M) = \min\{\xi(g), \xi(h)\}.$$

Again, for $g, h \in G$, let M be the smallest group containing g, let N be the smallest group containing h, and let P be the smallest group in $\mathscr{B} \cup \{G\}$ containing $\{[m, n] \mid m \in M, n \in N\}$. Then, since $[g, h] \in P$,

$$\xi([g, h]) \geqslant \rho(P) \geqslant \rho(M) + \rho(N) = \xi(g) + \xi(h).$$

Also,

$$\begin{aligned} \xi(g) = \rho(M) &\leqslant \min\{\nu(p)/\varphi(\text{order}(m)) \mid m \in M\} \\ &\leqslant \nu(p)/\varphi(\text{order}(g)), \end{aligned}$$

since $g \in M$. Suppose now that $(\mathscr{B}, \rho)$ is p-adic. If $g \in G$, let M be the smallest group in $\mathscr{B} \cup \{G\}$ containing g and let N be the smallest group in $\mathscr{B} \cup \{G\}$ containing $\{m^p \mid m \in M\}$. Then, since $g^p \in N$,

$$\xi(g^p) \geqslant \rho(N) \geqslant p\rho(M) = p\xi(g).$$

Therefore, in this case, ξ is p-adic. Denote the group valuation ξ we have constructed from $(\mathscr{B}, \rho)$ by $\mathbf{X}(\mathscr{B}, \rho)$.

PROPOSITION 1.12. *The maps* **F** *and* **X** *define a one–one correspondence between the set of order-bounded group valuations on G and the set of strict weighted filtrations. The p-adic group valuations correspond to the p-adic weighted filtrations.*

Proof. We need only show that **F** and **X** are inverse to each other. Let ξ be an order-bounded group valuation. If $\xi' = \mathbf{XF}(\xi)$, then

$$\begin{aligned}\xi'(g) &= \max\{\rho(N) \mid g \in N\}\\ &= \max\{\rho(G_x) \mid g \in G_x\}.\end{aligned}$$

Since $\xi(g) \geqslant \rho(G_x) \geqslant x$ if $g \in G_x$, and $g \in G_x$ for all $x \leqslant \xi(g)$, it follows that $\mathbf{XF}(\xi) = \xi$.

Let $(\mathscr{B}, \rho)$ be a strict weighted filtration. Let $\xi = \mathbf{X}(\mathscr{B}, \rho)$, and let $(\mathscr{B}', \rho') = \mathbf{F}(\xi)$. Note that from the definition of ξ and from the fact that $(\mathscr{B}, \rho)$ is strict, $g \in N$ if and only if $\xi(g) \geqslant \rho(N)$. Therefore, $N = G_{\rho(N)}$, so $\mathscr{B} \subseteq \mathscr{B}'$. Since $\mathscr{B}' = \{G_x \mid x \in \text{Range } \xi\}$, and Range ξ = Range ρ, it follows that, actually, $\mathscr{B} = \mathscr{B}'$. We now show that $\rho = \rho'$. Note first that for each $N \in \mathscr{B}$, there exists $g_0 \in N$ such that g_0 is not in any smaller group in $\mathscr{B}$. Then,

$$\xi(g_0) = \max\{\rho(M) \mid g_0 \in M\} = \rho(N).$$

Also,

$$\rho'(N) = \min\{\xi(g) \mid g \in N\} \leqslant \xi(g_0) = \rho(N).$$

If $\rho'(N) < \rho(N)$, then for some $g_1 \in N$, $\xi(g_1) < \rho(N)$. Since

$$\xi(g_1) = \max\{\rho(M) \mid g_1 \in M\},$$

this is impossible. Therefore, $\rho = \rho'$, which shows that $\mathbf{FX}(\mathscr{B}, \rho) = (\mathscr{B}, \rho)$. This completes the proof of the proposition.

We will now discuss the relation between weighted filtrations and quotient groups. Let G be a finite group, let H be a normal subgroup of G, and let $q\colon G \to G/H$ be the map of G onto the quotient group. If $(\mathscr{B}, \rho)$ is a weighted filtration in G, let

$$\mathscr{B}' = \{q(M) \mid M \in \mathscr{B}\}$$

and let $\rho'\colon \mathscr{B}' \to \mathbf{R} \cup \{\infty\}$ be defined by

$$\rho'(M') = \max\{\rho(M) \mid q(M) = M'\}.$$

DEFINITION 1.13. $(\mathscr{B}, \rho)/H = (\mathscr{B}', \rho')$ is the *quotient of* $(\mathscr{B}, \rho)$ *by* H.

LEMMA 1.14. *$(\mathscr{B}, \rho)/H$ is a weighted filtration in G/H. If $(\mathscr{B}, \rho)$ is strict, then $(\mathscr{B}, \rho)/H$ is strict. If $(\mathscr{B}, \rho)$ is complete, then $(\mathscr{B}, \rho)/H$ is complete. If $(\mathscr{B}, \rho)$*

is p-adic, then $(\mathscr{B}, \rho)/H$ *is p-adic. If* $(\mathscr{B}_1, \rho_1)$ *is a trivial extension of* $(\mathscr{B}, \rho)$, *then* $(\mathscr{B}_1, \rho_1)/H$ *is a trivial extension of* $(\mathscr{B}, \rho)/H$.

Proof. It is immediate that $\mathscr{B}'$ is a filtration base and that ρ' is a positive valued order-reversing function from $\mathscr{B}'$ to $\mathbf{R} \cup \{\infty\}$ such that $\rho'(M') = \infty$ if and only if $M' = \{1\}$. Let $M', N' \in \mathscr{B}'$, and let P' be the smallest group in $\mathscr{B}'$ containing $\{[m, n] \mid m \in M', n \in N'\}$. Let M be the smallest group in $\mathscr{B}$ such that $q(M) = M'$, let N be the smallest group in $\mathscr{B}$ such that $q(N) = N'$, and let Q be the smallest group in $\mathscr{B}$ containing $\{[m, n] \mid m \in M, n \in N\}$. Then, $q(Q) \supseteq q([M, N]) = [M', N']$. Therefore, $q(Q) \supseteq P'$, so

$$\begin{aligned}\rho'(P') &\geqslant \rho'(q(Q)) \geqslant \rho(Q)\\ &\geqslant \rho(M) + \rho(N) = \rho'(M') + \rho'(N').\end{aligned}$$

Also,

$$\begin{aligned}\rho'(M') &= \rho(M),\\ &\leqslant \min\{\nu(p)/\varphi(\mathrm{order}(m)) \mid m \in M\}\\ &\leqslant \min\{\nu(p)/\varphi(\mathrm{order}(q(m))) \mid m \in M\}\\ &= \min\{\nu(p)/\varphi(\mathrm{order}(m')) \mid m' \in M'\}.\end{aligned}$$

Suppose now that $(\mathscr{B}, \rho)$ is p-adic. Let $M' \in \mathscr{B}'$ and let M be the smallest group in $\mathscr{B}$ with $q(M) = M'$. If N is the smallest group in $\mathscr{B}$ containing $\{m^p \mid m \in M\}$ and N' is the smallest group in $\mathscr{B}'$ containing $\{m'^p \mid m' \in M'\}$, then $q(N) \supseteq N'$. Now,

$$\rho'(N') \geqslant \rho'(q(N)) \geqslant \rho(N) \geqslant p\rho(M) = p\rho'(M').$$

Therefore, $(\mathscr{B}, \rho)/H$ is p-adic. It is immediate that if $(\mathscr{B}, \rho)$ is complete, then $(\mathscr{B}, \rho)/H$ is complete. Suppose now that $(\mathscr{B}, \rho)$ is strict. If $(\mathscr{B}, \rho)/H$ were not strict, then $\rho'(M') = \rho'(N')$ for some $M' \neq N'$ in $\mathscr{B}'$. But $\rho'(M') = \rho(M)$ for M the smallest group in $\mathscr{B}$ with $q(M) = M'$, and $\rho'(N') = \rho(N)$ for N the smallest group in $\mathscr{B}$ with $q(N) = N'$. This implies that $\rho(M) = \rho(N)$, which is impossible since $M \neq N$ and $(\mathscr{B}, \rho)$ is strict. Therefore, if $(\mathscr{B}, \rho)$ is strict, then $(\mathscr{B}, \rho)/H$ is strict also.

Suppose now that $(\mathscr{B}_1, \rho_1)$ is a trivial extension of $(\mathscr{B}, \rho)$. If $(\mathscr{B}_1, \rho_1)/H = (\mathscr{B}_1', \rho_1')$, it is immediate that $\mathscr{B}_1' \supseteq \mathscr{B}'$. We now show that

$$\rho_1'(N_1') = \max\{\rho'(N') \mid N' \supseteq N_1'\}$$

by showing that if N' is the smallest group in $\mathscr{B}'$ containing N_1', then $\rho_1'(N_1') = \rho'(N')$. Let N_1 be the smallest group in $\mathscr{B}_1$ with $q(N_1) = N_1'$, let N be the smallest group in $\mathscr{B}$ with $q(N) = N'$, and let M be the smallest group in $\mathscr{B}$ containing N_1. Then,

$$\rho'(N') = \rho(N)$$

and

$$\rho_1'(N') = \rho_1(N_1) = \rho(M).$$

Since $q(M) \supseteq q(N_1) = N_1'$, it follows that $q(M) \supseteq N'$. Therefore, $M \supseteq N$. If $N \subset N_1$, then $q(N) = q(N_1)$, which would contradict the choice of N_1 as the smallest group in $\mathscr{B}_1 \supseteq \mathscr{B}$ mapping onto N_1'. Therefore, $N \supseteq N_1$. But M is the smallest group in $\mathscr{B}$ containing N_1. Therefore, $M = N$. Therefore, $\rho_1'(N_1') = \rho(M) = \rho(N) = \rho'(N')$. This proves that $(\mathscr{B}_1', \rho_1')$ is a trivial extension of $(\mathscr{B}', \rho')$. This completes the proof of the lemma.

It is easy to describe the quotient of a weighted filtration in the special case in which the normal subgroup H is contained between two successive subgroups in $\mathscr{B}$: Suppose $\mathscr{B} = \{N_i \mid i = 0,..., k\}$, with $N_0 = \{1\}$, $N_i \subset N_{i+1}$, and $N_r \subseteq H \subset N_{r+1}$. Then, if $(\mathscr{B}, \rho)/H = (\mathscr{B}', \rho')$, we have $\mathscr{B}' = \{N_i' \mid i = r,..., k\}$, where $N_r' = \{1\}$, and $N_i' = N_i/H$ and $\rho'(N_i') = \rho(N_i)$ for $i = r + 1,..., k$.

In Proposition 1.12, it was stated that there is a one-one correspondence between order-bounded group valuations and strict weighted filtrations. More generally, it can be shown that if $(\mathscr{B}_1, \rho_1)$ and $(\mathscr{B}_2, \rho_2)$ are two filtrations, then $\mathbf{X}(\mathscr{B}_1, \rho_1) = \mathbf{X}(\mathscr{B}_2, \rho_2)$ if and only if there exists a strict weighted filtration $(\mathscr{B}, \rho)$ such that $(\mathscr{B}_1, \rho_1)$ and $(\mathscr{B}_2, \rho_2)$ are both trivial extensions of $(\mathscr{B}, \rho)$. We could define an equivalence relation between weighted filtrations by saying that two weighted filtrations are equivalent if they are both trivial extensions of the same strict weighted filtration. If $(\mathscr{B}, \rho)$ is an arbitrary weighted filtration, then $\mathbf{FX}(\mathscr{B}, \rho)$ is the unique strict weighted filtration of which it is a trivial extension. The functions $\mathbf{F}$ and $\mathbf{X}$ give a one-one correspondence between group valuations and equivalence classes of weighted filtrations. It follows from Lemma 1.14 that taking quotients of weighted filtrations preserves this equivalence relation.

2. Hopf Algebras and Integral Orders

In this section, we introduce the notion of an integral order in a Hopf algebra. An important invariant associated with the integral order A is the ideal $\epsilon(L_A)$, where

$$L_A = \{x \in A \mid ax = \epsilon(a)x, \text{ for all } a \in A\}.$$

For a detailed discussion of integral orders in general, and specifically of the significance of $\epsilon(L_A)$, see [8]. The chief result in this section is that $\epsilon(L_A)$ is multiplicative.

By a *bialgebra* over R, we mean a quintuple $(A, \mu, \eta, \delta, \epsilon)$ such that A is a finitely generated projective R-module, (A, μ, η) is a R-algebra, (A, δ, ϵ) is a R-coalgebra, and δ and ϵ are algebra maps. If there exists a map $\sigma\colon A \to A$ satisfying

$$\eta\epsilon = \mu(\sigma \otimes I)\delta = \mu(I \otimes \sigma)\delta,$$

we say that A (or more precisely $(A, \mu, \eta, \delta, \epsilon)$) is a *Hopf algebra* over R with *antipode* σ. A is called *involutory* if $\sigma^2 = I$. An element $\Lambda \in A$ is called a *left integral* if $a\Lambda = \epsilon(a)\Lambda$ for all $a \in A$. Denote by L_A the two-sided ideal of all left integrals in A. A Hopf algebra A over R is called a *Hopf algebra order* in a Hopf algebra H over k if $k \otimes_R A \cong H$.

If G is a finite group, kG is a Hopf algebra over k, where $\delta(g) = g \otimes g$ and $\epsilon(g) = 1$ for all $g \in G$. RG is a Hopf algebra order in kG. $L_{RG} = \{r \sum g \mid r \in R\}$. Note that $\epsilon(L_{RG}) = |G| R$.

Let $f\colon H_1 \to H$ be an injective Hopf algebra morphism. The morphism f is called *normal* if

$$f(H_1{}^+)H = Hf(H_1{}^+),$$

where $H_1{}^+$ denotes the augmentation ideal of H_1. If f is normal, then $H/f(H_1{}^+)H$ is a quotient Hopf algebra of H; the Hopf algebra morphism $H \to H/f(H_1{}^+)H$ is called the *cokernel* of f. Let $g\colon H \to H_2$ be a surjective Hopf algebra morphism. The morphism g is called *conormal* if

$$\{x \mid (g \otimes I)\, \delta(x) = 1 \otimes x\} = \{x \mid (I \otimes g)\, \delta(x) = x \otimes 1\}.$$

If g is conormal, then this set is a sub-Hopf algebra of H (see [15, Chap. 16]). The injection morphism of this sub-Hopf alegbra into H is called the *kernel* of g. A *short exact sequence* of Hopf algebras is a sequence

$$H_1 \xrightarrow{f} H \xrightarrow{g} H_2,$$

where f is normal with cokernel g, and g is conormal with kernel f. Note that if H is finite dimensional, then H_1 and H_2 are also finite dimensional and that

$$H_2{}^* \xrightarrow{g^*} H^* \xrightarrow{f^*} H_1{}^*$$

is also a short exact sequence. More details on questions of extensions of Hopf algebras in various contexts can be found in [1, 2, 10–16, 19].

The chief result of this section is

PROPOSITION 2.1. *Let $H' \xrightarrow{f} H \xrightarrow{g} H''$ be a short exact sequence of finite-dimensional involutory Hopf algebras over k such that* $\dim_k H = (\dim_k H')(\dim_k H'')$, *and let A be a Hopf algebra order in H. If $A' = f^{-1}(A)$ and $A'' = g(A)$, then, A' is a Hopf algebra order in H', A'' is a Hopf algebra order in H'', and*

$$\epsilon(L_A) = \epsilon(L_{A'})\, \epsilon(L_{A''}).$$

Proof. Theorem 4.3 of [7] implies that H, H^*, H', H'^*, H'', and H''^* are all semisimple. The assertion that A' is a Hopf algebra order follows from the fact that $A' \cong f(A') = f(H') \cap A$. Since $f(H') \cap A$ is a R-module direct summand of A, the various conditions that must be satisfied for $f(H') \cap A$ to be a Hopf algebra order in $f(H')$ are easily checked. It is also clear that A'' is a Hopf algebra order in H''.

We first show that $\epsilon(L_A)$ divides $\epsilon(L_{A'})\,\epsilon(L_{A''})$. To show this, it is sufficient to show for each prime ideal $P \subset R$ that $\epsilon(L_A)\,R_P$ divides $\epsilon(L_{A'})\,\epsilon(L_{A''})\,R_P$. Therefore, we may localize R at P and assume that R is a principal ideal domain. By [9], A' has a nonsingular left integral Λ', A has a nonsingular left integral Λ, and A'' has a nonsingular left integral Λ''. Let $\Lambda_1'' \in A$ satisfy $g(\Lambda_1'') = \Lambda''$. We will show that $\Lambda_1'' f(\Lambda')$ is a left integral in A. Since

$$g(a\Lambda_1'') = g(a)\,\Lambda'' = \epsilon(g(a))\,\Lambda'' = \epsilon(a)\,\Lambda'',$$

it follows that

$$a\Lambda_1'' = \epsilon(a)\,\Lambda_1'' + c,$$

where $c \in \operatorname{Ker} g = Hf(H'^+)$. Therefore,

$$a\Lambda_1'' f(\Lambda') = \epsilon(a)\,\Lambda_1'' f(\Lambda') + cf(\Lambda'),$$

and since

$$Hf(H'^+)f(\Lambda') = Hf(H'^+\Lambda') = Hf(0) = 0,$$

it follows that

$$a\Lambda_1'' f(\Lambda') = \epsilon(a)\,\Lambda_1'' f(\Lambda').$$

Therefore, $\Lambda_1'' f(\Lambda')$ is a left integral in A. By [9], $\Lambda_1'' f(\Lambda') = r\Lambda$ for some r in R. Therefore, $\epsilon(\Lambda_1'')\,\epsilon f(\Lambda') = r\epsilon(\Lambda)$, which implies that $\epsilon(\Lambda'')\,\epsilon(\Lambda') = r\epsilon(\Lambda)$. Therefore, $\epsilon(L_A)$ divides $\epsilon(L_{A'})\,\epsilon(L_{A''})$.

The sequence

$$H''^* \xrightarrow{g^*} H^* \xrightarrow{f^*} H'^*,$$

is a short exact sequence of Hopf algebras and A^* is a Hopf algebra order in H^*. Note that

$$\begin{aligned} A''^* &= \{x \in H''^* \mid x(A'') \subseteq R\} \\ &= \{x \in H''^* \mid x(g(A)) \subseteq R\} \\ &= \{x \in H''^* \mid g^*(x)(A) \subseteq R\} \\ &= \{x \in H''^* \mid g^*(x) \in A^*\} \\ &= g^{*-1}(A^*), \end{aligned}$$

and that

$$\begin{aligned} A'^* &= \{x \in H'^* \mid x(A') \subseteq R\} \\ &= \{f^*(y) \mid f^*(y)(A') \subseteq R\} \\ &= \{f^*(y) \mid y(f(A')) \subseteq R\} \\ &= \{f^*(y) \mid y(A) \subseteq R\} \\ &= f^*(A^*). \end{aligned}$$

The next to the last equality follows from the fact that $f(A')$ is a direct summand of the R-module A. Therefore, applying the first part of the proof to the short exact sequence

$$H''^* \to H^* \to H'^*$$

and to the order A^* we get that $\epsilon(L_{A^*})$ divides $\epsilon(L_{A''^*})\,\epsilon(L_{A'^*})$. By [7, Proposition 2.2],

$$\epsilon(L_{A''^*}) = (\dim_k H'')\,\epsilon(L_{A''})^{-1},$$
$$\epsilon(L_{A^*}) = (\dim_k H)\,\epsilon(L_A)^{-1},$$

and

$$\epsilon(L_{A'^*}) = (\dim{}_k H')\,\epsilon(L_{A'})^{-1}.$$

Since $\dim_k H = (\dim_k H'')(\dim_k H')$, we have that $(\dim_k H)\,\epsilon(L_A)^{-1}$ divides $(\dim_k H)\,\epsilon(L_{A''})^{-1}\,\epsilon(L_{A'})^{-1}$. Therefore, $\epsilon(L_{A'})\,\epsilon(L_{A''})$ divides $\epsilon(L_A)$. This completes the proof of the proposition.

3. Orders and Valuations

In this section, we describe a correspondence between Hopf algebra orders and p-adic order-bounded group valuations. We give an explicit description of the R-module basis of an order arising from a p-adic valuation in the case that R is a principal ideal domain. We also discuss the relation between the valuation associated with the order A and the structure of the Hopf algebra $\bar{k} \otimes_R A$ over the residue class field $\bar{k}$.

Let ν be a valuation on k, let G be a finite group, and let A be a Hopf algebra order in kG. We will construct a group valuation $\xi = \Xi(A)$, which is order bounded with respect to ν and p-adic, as follows: For $g \neq 1$, let

$$I_g = \{x \in k \mid x(g-1) \in A\}.$$

It is easily checked that I_g is a fractional ideal in k. It is shown in [5, first paragraph of the proof of theorem], that $RG \subseteq A$. This implies that $I_g \supseteq R$. Therefore, $I_g^{-1} \subseteq R$. Let

$$\xi(g) = \nu(I_g^{-1}), \qquad \text{if} \qquad g \neq 1,$$
$$\xi(1) = \infty.$$

It is immediate that for $g \neq 1$, $\xi(g)$ is a nonnegative real number. From the fact that

$$gh - 1 = (g-1)h + (h-1),$$

it follows that

$$I_{gh} \supseteq I_g \cap I_h .$$

Therefore,

$$I_{gh}^{-1} \subseteq (I_g \cap I_h)^{-1} = I_g^{-1} + I_h^{-1}.$$

This implies that

$$\begin{aligned} \xi(gh) &= \nu(I_{gh}^{-1}) \\ &\geqslant \nu(I_g^{-1} + I_h^{-1}) \\ &= \min\{\nu(I_g^{-1}), \nu(I_h^{-1})\} \\ &= \min\{\xi(g), \xi(h)\}. \end{aligned}$$

Note that

$$\begin{aligned} [g, h] - 1 &= ghg^{-1}h^{-1} - 1 \\ &= (gh - hg)\, g^{-1}h^{-1} \\ &= ((g-1)(h-1) - (h-1)(g-1))\, g^{-1}h^{-1}. \end{aligned}$$

It follows from this that

$$I_{[g,h]} \supseteq I_g I_h .$$

Therefore,

$$I_{[g,h]}^{-1} \subseteq I_g^{-1} I_h^{-1},$$

which implies that

$$\begin{aligned} \xi([g, h]) &= (I_{[g,h]}^{-1}) \\ &\geqslant \nu(I_g^{-1}) + \nu(I_h^{-1}) \\ &= \xi(g) + \xi(h). \end{aligned}$$

Replacing k by a finite extension if necessary, we may assume that k contains a primitive $|G|$th root of unity. Consider an element g of G and suppose $m = \text{order}(g)$. We can find a basis $\{a_1, \ldots, a_k\}$ of kG such that $a_i g = \theta_i a_i$, where θ_i is a mth root of unity. All of the mth roots of unity appear among the θ_i since they all appear among the roots of the characteristic polynomial of the linear transformation $a \mapsto ag$. Now, $a_i I_g(g-1) = I_g(\theta_i - 1)\, a_i$. Since $I_g(g-1) \subseteq A$ and A is a finitely generated R-module, $I_g(\theta_i - 1)$ is an integral ideal. If m is not a prime power, it follows from [18, Proposition 7-6-2(ii)] that $I_g = R$. If $m = q^s$, with q prime, let θ be a primitive

mth root of unity. Then, $I_g(\theta - 1) \subseteq R$ implies $R(\theta - 1) \subseteq I_g^{-1}$. It follows that $\nu(I_g^{-1}) \leqslant \nu(\theta - 1)$. By [18, Proposition 7-4-1], we have that $\nu(\theta - 1) = \nu(q)/\varphi(q^s)$. Therefore, in this case, $\xi(g) \leqslant \nu(q)/\varphi(\text{order}(g))$. Therefore, ξ is order bounded with respect to ν.

Let p be the rational prime for which $\nu(p) \neq 0$. If order(g) is not a power of p, then order(g^p) is not a power of p, so $\xi(g^p) = p\xi(g) = 0$. Suppose now that order$(g) = p^s$. If $s = 1$, then

$$\xi(g^p) = \xi(1) = \infty \geqslant p\xi(g).$$

Suppose that $s > 1$. From

$$\xi(g) \leqslant \nu(p)/(p-1)\,p^{s-1} < \nu(p)/(p-1),$$

it follows that

$$(p-1)\,\nu(I_g^{-1}) < \nu(p).$$

Therefore,

$$p\nu(I_g^{-1}) < \nu(I_g^{-1}) + \nu(p) < i\nu(I_g^{-1}) + \nu(p),$$

for $i = 1,\ldots, p-1$. Therefore,

$$\nu(I_g^{-p}) < \nu(pI_g^{-i}).$$

Since $\nu(C_{p,i}) = \nu(p)$ for $i = 1,\ldots, p-1$, we have

$$\nu(I_g^{-p}) < \nu(C_{p,i}I_g^{-i}).$$

This implies that

$$\nu\left(\sum_{i=1}^{p-1} C_{p,i}I_g^{-i} + I_g^{-p}\right) = \nu(I_g^{-p}) = p\xi(g).$$

Denote g^p by h. Then, from

$$g^p = ((g-1)+1)^p = \sum_{i=0}^{p} C_{p,i}(g-1)^i,$$

we get

$$h - 1 = g^p - 1 = \sum_{i=1}^{p-1} C_{p,i}(g-1)^i + (g-1)^p.$$

It follows that

$$I_h \supseteq \bigcap_{i=1}^{p-1} (1/C_{p,i})\, I_g{}^i \cap I_g{}^p,$$

so

$$I_h^{-1} \subseteq \sum_{i=1}^{p-1} C_{p,i} I_g^{-i} + I_g^{-p}.$$

Therefore,

$$\begin{aligned}\xi(g^p) &= \nu(I_h^{-1}) \\ &\geqslant \nu\left(\sum_{i=1}^{p-1} C_{p,i} I_g^{-i} + I_g^{-p}\right) \\ &= p\xi(g).\end{aligned}$$

We have proved:

PROPOSITION 3.1. *Let ν be a valuation on k, let G be a finite group, and let A be a Hopf algebra order in kG. Let*

$$I_g = \{x \in k \mid x(g-1) \in A\}, \qquad \textit{for} \quad g \neq 1$$

and define $\xi = \Xi(A)$ by

$$\begin{aligned}\xi(g) &= \nu(I_g^{-1}), \qquad \textit{for } g \neq 1, \\ \xi(1) &= \infty.\end{aligned}$$

Then, ξ is a p-adic order-bounded group valuation on G. If A_1 and A_2 are Hopf algebra orders with $A_1 \subseteq A_2$, then $\Xi(A_1) \leqslant \Xi(A_2)$.

We now construct a Hopf algebra order from an order-bounded group valuation. Let x be in the range of the valuation ν. Denote by $\mathfrak{P}^x$ the ideal in k that satisfies

$$\nu(\mathfrak{P}^x) = x,$$

and

$$\nu'(\mathfrak{P}^x) = 0, \qquad \text{for all valuations } \nu' \text{ not equivalent to } \nu.$$

PROPOSITION 3.2. *Let ν be a valuation on k, let G be a finite group, and let ξ be a group valuation on G that is order bounded with respect to ν. Let $A = \mathbf{A}(\xi)$ be the R-subalgebra of kG generated by $\mathfrak{P}^{-\xi(g)}(g-1)$, for all $g \neq 1$. Then, A is a Hopf algebra order in kG. If ξ_1 and ξ_2 are order-bounded group valuations with $\xi_1 \leqslant \xi_2$, then, $\mathbf{A}(\xi_1) \subseteq \mathbf{A}(\xi_2)$.*

Proof. We need show only that A is a finitely generated R-module, that $\delta(A) \subseteq A \otimes_R A$, and that $\sigma(A) \subseteq A$.

We first show that A is a finitely generated R-module. First consider the case where $\xi(g) > 0$ for all g in G. Pick a fixed linear ordering of the elements of G such that $\xi(g) \leqslant \xi(h)$ if $g > h$. For each g in G, let A_g be the R-algebra generated by $\mathfrak{P}^{-\xi(g)}(g-1)$ in $k\langle g\rangle$. We will show that A is finitely generated by showing first, that the map

$$t: A_g \otimes_R A_h \otimes_R \cdots \otimes_R A_k \to A,$$

where $g < h < \cdots < k$ is a listing of all the elements of G in order, defined by

$$t(a_g \otimes a_h \otimes \cdots \otimes a_k) = a_g a_h \cdots a_k, \qquad a_i \in A_i,$$

is surjective, and second, that each A_g is a finitely generated R-module. Observe that A is spanned by R-submodules of the form

$$\mathfrak{P}^{-\xi(g)}(g-1)\,\mathfrak{P}^{-\xi(h)}(h-1)\cdots\mathfrak{P}^{-\xi(k)}(k-1).$$

Call such a submodule a *monomial* submodule. Call a monomial submodule *straight* if $g \leqslant h \leqslant \cdots \leqslant k$ in the chosen ordering of G. Call a monomial submodule g_0-*initial* if $g, h,..., k \leqslant g_0$. To show that the map t is surjective it is sufficient to show that every monomial submodule is contained in the span of straight monomial submodules. Since the set G is finite, the chosen linear ordering is, of course, a well ordering. We will show by induction that every g_0-initial monomial submodule is contained in the span of g_0-initial straight monomial submodules. It is clear that this holds if g_0 is the first element in G. Now, let g_0 be an arbitrary element of G and suppose that for every $h < g_0$, every h-initial monomial submodule is contained in the span of h-initial straight monomial submodules. Denote $m' = [g_0, m]$. Since $g_0 m = m' m g_0$, we have

$$\begin{aligned}(g_0-1)(m-1) &= m'(mg_0 - g_0 - m + 1)\\ &\quad + (m'-1)g_0 + (m'-1)m - (m'-1)\\ &= (m-1)(g_0-1) + (m'-1)(m-1)(g_0-1)\\ &\quad + (m'-1)(g_0-1) + (m'-1)(m-1) + (m'-1).\end{aligned}$$

Since, by hypothesis, $\xi(g_0), \xi(m) > 0$, we have

$$\xi(m') \geqslant \xi(g_0) + \xi(m) > \xi(g_0), \xi(m)$$

and so, $m' < g_0, m$. Suppose that $m < g_0$. Then,

$$\begin{aligned}&\mathfrak{P}^{-\xi(g_0)}(g_0-1)\,\mathfrak{P}^{-\xi(m)}(m-1)\\ &\quad\subseteq \mathfrak{P}^{-\xi(m)}(m-1)\,\mathfrak{P}^{-\xi(g_0)}(g_0-1)\\ &\qquad + \mathfrak{P}^{\xi(m')}(\mathfrak{P}^{-\xi(m')}(m'-1)\,\mathfrak{P}^{-\xi(m)}(m-1)\,\mathfrak{P}^{-\xi(g_0)}(g_0-1))\\ &\qquad + \mathfrak{P}^{\xi(m')-\xi(m)}(\mathfrak{P}^{-\xi(m')}(m'-1)\,\mathfrak{P}^{-\xi(g_0)}(g_0-1))\\ &\qquad + \mathfrak{P}^{\xi(m')-\xi(g_0)}(\mathfrak{P}^{-\xi(m')}(m'-1)\,\mathfrak{P}^{-\xi(m)}(m-1))\\ &\qquad + \mathfrak{P}^{\xi(m')-\xi(g_0)-\xi(m)}(\mathfrak{P}^{-\xi(m')}(m'-1)).\end{aligned}$$

Using repeated applications of this relation, we see that any g_0-initial monomial submodule is contained in the span of g_0-initial monomial submodules such that in each monomial submodule, the $(g_0 - 1)$-factors all appear at the right-hand end of the monomial. By induction, the parts of the monomials to the left of the $(g_0 - 1)$-factors lie in the span of straight monomial submodules; multiplying these straight monomial submodules on the right by suitable $(g_0 - 1)$-factors will not change the straightness. Therefore, every g_0-initial monomial submodule lies in a span of g_0-initial straight monomial submodules. This proves that the map t is surjective.

We now show that each A_g is a finitely generated R-module. Since $\xi(g) > 0$, $\operatorname{order}(g) = p^s$ for some s. For some finite extension K/k, $K\langle g\rangle \cong K \oplus \cdots \oplus K$ as algebras, and $\nu(p)/\varphi(p^s)$ is in the range of ν. Let S be the integral closure of R in K. Under the embedding $A_g \subseteq K\langle g\rangle$, the element g corresponds to $(\theta_1, \ldots, \theta_t)$ in $K \oplus \cdots \oplus K$, where each θ_i is a primitive p^rth root of unity, for some $r \leqslant s$ depending on i. By [18, Proposition 7-4-1], $S\mathfrak{P}^{\nu(p)/\varphi(p^r)}$ divides $S(\theta_i - 1)$. Since

$$\xi(g) \leqslant \nu(p)/\varphi(p^s) \leqslant \nu(p)/\varphi(p^r),$$

we have that

$$\mathfrak{P}^{-\xi(g)}(\theta_i - 1) \subseteq S.$$

Therefore, the isomorphic image of A_g in $K \oplus \cdots \oplus K$ sits in $S \oplus \cdots \oplus S$. Since S is a finitely generated R-module, it follows that A_g is a finitely generated R-module. This completes the proof that A is a finitely generated R-module, in the case that $\xi(g) > 0$ for all $g \neq 1$.

Now, let ξ be an arbitrary order-bounded group valuation on G and let $G_+ = \{g \in G \mid \xi(g) > 0\}$. Note that G_+ is a normal subgroup of G. By the previous case $A_+ = \mathbf{A}(\xi \mid G_+)$ is a finitely generated R-module in kG_+. From the fact that $\xi(hgh^{-1}) = \xi(g)$ it follows that $hA_+h^{-1} \subseteq A_+$. Therefore, $A = A_+RG$, which is a finitely generated R-module.

We now show that $\delta(A) \subseteq A \otimes_R A$. Since

$$\delta(g - 1) = (g - 1) \otimes 1 + 1 \otimes (g - 1) + (g - 1) \otimes (g - 1),$$

we have

$$\begin{aligned}\delta(\mathfrak{P}^{-\xi(g)}(g - 1)) \subseteq (\mathfrak{P}^{-\xi(g)}(g - 1)) \otimes 1 + 1 \otimes (\mathfrak{P}^{-\xi(g)}(g - 1)) \\ + \mathfrak{P}^{\xi(g)}(\mathfrak{P}^{-\xi(g)}(g - 1)) \otimes (\mathfrak{P}^{-\xi(g)}(g - 1)).\end{aligned}$$

Since δ is an algebra homomorphism and since A is generated by the submodules $\mathfrak{P}^{-\xi(g)}(g - 1)$, it follows that $\delta(A) \subseteq A \otimes_R A$. The proof that $\sigma(A) \subseteq A$ is similar and uses the fact that $\xi(g) = \xi(g^{-1})$, so that

$$\sigma(\mathfrak{P}^{-\xi(g)}(g - 1)) = \mathfrak{P}^{-\xi(g^{-1})}(g^{-1} - 1).$$

It is clear from the definition of $\mathbf{A}(\xi)$ that if $\xi_1 \leqslant \xi_2$, then $\mathbf{A}(\xi_1) \subseteq \mathbf{A}(\xi_2)$. This completes the proof of the proposition.

The following three corollaries are immediate:

COROLLARY 3.3. *Let ξ be an order-bounded group valuation on G and let $\xi' = \Xi\mathbf{A}(\xi)$. Then, $\xi' \geqslant \xi$.*

COROLLARY 3.4. *Let A be a Hopf algebra order in kG and let $A' = \mathbf{A}\Xi(A)$. Then, $A' \subseteq A$.*

COROLLARY 3.5. *The maps $\mathbf{A}$ and Ξ defined above satisfy $\mathbf{A}\Xi\mathbf{A} = \mathbf{A}$ and $\Xi\mathbf{A}\Xi = \Xi$.*

Proposition 1.7 is an immediate consequence of Corollary 3.3: Let ξ be a maximal order-bounded group valuation on G. Since ξ is maximal, $\xi = \Xi\mathbf{A}(\xi)$. But $\Xi\mathbf{A}(\xi)$ is p-adic.

We can gain some insight into the nature of the constructions in this section by considering in more detail what happens modulo the prime ideal P corresponding to ν. Let $\bar{k}$ be the residue class field modulo this prime. If A is a Hopf algebra order in kG, the embedding $RG \subseteq A$ induces a map $\bar{k}G \to \bar{k} \otimes_R A$ of Hopf algebras over $\bar{k}$. The kernel of this map (in the category of Hopf algebras over $\bar{k}$) is $\bar{k}G_+$, where $G_+ = \{g \in G \mid \xi(g) > 0\}$, and $\xi = \Xi(A)$. If H is a Hopf algebra, denote the set of grouplike elements of H by $\Gamma(H)$.

PROPOSITION 3.6. *If A is a Hopf algebra order in kG, then $\Gamma(\bar{k} \otimes_R A) \cong G/G_+$.*

Proof. It follows from the above discussion that the kernel of the map $G \to \Gamma(\bar{k} \otimes_R A)$ is G_+. We must show that this map is onto. Let h be an element of $\Gamma(\bar{k} \otimes_R A)$. We can think of h as an algebra homomorphism from

$$\bar{k} \otimes_R A^* = \bar{k} \otimes_R (\hom_R(A, R)) = \hom_{\bar{k}}(\bar{k} \otimes_R A, \bar{k})$$

to $\bar{k}$. Since $RG \subseteq A$, we have that $A^* \subseteq RG^* = \hom_R(RG, R)$. This inclusion induces a map

$$r: \bar{k} \otimes_R A^* \to \bar{k} \otimes_R RG^* = \bar{k}G^*.$$

We must show that the map $h: \bar{k} \otimes_R A^* \to \bar{k}$ factors through the map r. We first show that $\operatorname{Ker} r = \operatorname{Rad}(\bar{k} \otimes_R A^*)$. We identify $\bar{k} \otimes_R A^*$ with A^*/PA^* and $\bar{k}G^*$ with RG^*/PRG^*.

Suppose $\bar{x} = x + PA^*$ is in $\operatorname{Ker} r$. This says that x is in PRG^*. Since $P^tRG^* \subseteq A^*$ for some t by [8, Proposition 3.1], $P^{t+1}RG^* \subseteq PA^*$ so $\bar{x}^{t+1} = 0$.

Therefore, $\operatorname{Ker} r$ is a nil ideal, so $\operatorname{Ker} r \subseteq \operatorname{Rad}(\bar{k} \otimes_R A^*)$. Since $\bar{k}G^*$ is a commutative separable $\bar{k}$-algebra, $r(\operatorname{Rad}(\bar{k} \otimes_R A^*)) = 0$, so

$$\operatorname{Rad}(\bar{k} \otimes_R A^*) \subseteq \operatorname{Ker} r.$$

Since h induces an algebra homomorphism from $B = \bar{k} \otimes_R A^*/\operatorname{Rad}(\bar{k} \otimes_R A^*)$ to $\bar{k}$, and since B is a finite-dimensional semisimple algebra, there exists e in $\bar{k} \otimes_R A^*$ such that $h(e) = 1$, $e(\operatorname{Ker} h) \subseteq \operatorname{Rad}(\bar{k} \otimes_R A^*)$, $e \notin \operatorname{Rad}(\bar{k} \otimes_R A^*)$, $e^2 - e \in \operatorname{Rad}(\bar{k} \otimes_R A^*)$. Since $\operatorname{Ker} r = \operatorname{Rad}(\bar{k} \otimes_R A^*)$, $r(e) \neq 0$. Also, $r(e)^2 = r(e^2) = r(e)$, and $r(e)\, r(\operatorname{Ker} h) = 0$. Therefore, there exists an algebra homomorphism $g\colon \bar{k}G^* \to \bar{k}$ such that $gr(e) \neq 0$, and $gr(\operatorname{Ker} h) = 0$. Since $gr(e)^2 = gr(e)$, it follows that $gr(e) = 1$. We now show that $gr = h$. Let x be in $\bar{k} \otimes_R A^*$. We can write $x = te + x'$, where $t \in \bar{k}$, and $x' \in \operatorname{Ker} h$. Then, $gr(x) = gr(te) + gr(x') = tgr(e) + 0 = t = h(x)$. Since $g\colon \bar{k}G^* \to \bar{k}$ is an algebra homomorphism, g is in $\Gamma(\bar{k}G) = G$. Since $gr = h$, g maps to h under the map $\bar{k}G \to \bar{k} \otimes_R A$. This completes the proof of the proposition.

Let $A_+ = A \cap kG$. We see that A_+ is a Hopf algebra order in kG_+. Since $\Gamma(\bar{k} \otimes_R A_+) = \{1\}$, $\bar{k} \otimes_R A_+$ is a pointed irreducible cocommutative Hopf algebra over $\bar{k}$. Also, $\bar{k} \otimes_R A$ is a split cocommutative Hopf algebra over $\bar{k}$. Note that the map $\bar{k} \otimes_R A_+ \to \bar{k} \otimes_R A$ is an injection since A_+ is a R-module direct summand of A. The action of G on G_+ via conjugation induces an action of G on $\bar{k} \otimes_R A_+$; since $\xi([g, h]) > \xi(h)$ if $g \in G_+$, this action is such that G_+ acts trivially on $\bar{k} \otimes_R A_+$. The induced action of G/G_+ on $\bar{k} \otimes_R A_+$ is just the action induced by the isomorphism $G/G_+ \cong \Gamma(\bar{k} \otimes_R A)$ and by the embedding $\bar{k} \otimes_R A_+ \subseteq \bar{k} \otimes_R A$, where $\Gamma(\bar{k} \otimes_R A)$ acts on $\bar{k} \otimes_R A$ via conjugation. An application of the structure theory of split cocommutative Hopf algebras (as found, for example, in [15, Chap. 8]) yields:

PROPOSITION 3.7. *Let A be a Hopf algebra order in kG. Then*

$$\bar{k} \otimes_R A = \bar{k} \otimes_R A_+ \# \bar{k}G/G_+.$$

As a consequence of this we get:

COROLLARY 3.8. *Let A be a Hopf algebra order in $\bar{k}G$. Then*

$$R \to A_+ \to A \to RG/G_+ \to R$$

is a short exact sequence of Hopf algebras over R. In particular,

$$A = A_+ RG \cong A_+ \otimes_{RG_+} RG.$$

We now consider the special case where $A = \mathbf{A}(\xi)$ for some order-bounded group valuation ξ. In this case, A is generated by elements of the monomial submodules $\mathfrak{P}^{-\xi(g)}(g - 1)$.

Since

$$\begin{aligned}\delta(t(g-1)) &= t(g-1)\otimes 1 + 1\otimes t(g-1)\\ &\qquad + t^{-1}t(g-1)\otimes t(g-1), \qquad \text{if} \quad \nu(t)<0,\\ &= tg\otimes g - t1\otimes 1, \qquad \text{if} \quad \nu(t)\geqslant 0,\end{aligned}$$

we see that $\bar{k}\otimes_R A$ is generated by primitive and grouplike elements. If $\xi(g)>0$, then $t(g-1)\in P\mathfrak{P}^{-\xi(g)}(g-1)$ for $\nu(t)\geqslant 0$, so $\bar{k}\otimes_R A_+$ is generated by primitive elements.

The above discussion makes it easy to provide many examples of Hopf algebra orders in kG that are not equal to $\mathbf{A}(\xi)$ for any group valuation ξ. Any order that is not generated by grouplikes and primitives modulo P is such an example. One such example is $(RZ_{p^n})^*\subsetneq (kZ_{p^n})^*\simeq kZ_{p^n}$ for $n>1$. Since $\bar{k}Z_{p^n}\simeq \bar{k}[X]/(X^{p^n})$, $\bar{k}\otimes_R (RZ_{p^n})^*$ has a sequence of divided powers up to p^n-1 and so is not primitively generated. Examples of this type raise the question of determining when $A=\mathbf{A}(\xi)$ for some ξ. The following example shows that it is not sufficient for $\bar{k}\otimes_R A_+$ to be primitively generated:

Example 3.9. Let R be the ring of integers in a suitably large algebraic number field and let ν be a valuation with $\nu(2)\neq 0$. Let G be the cyclic group of order 4. We will construct an order A in kG by giving a generating set for its dual order A^* in $kG^*=k\hat{G}$. Note that $\hat{G}$ is a cyclic group generated by the character χ. Pick positive numbers a, b in the range of ν such that $2a<b$, and $a+b<\nu(2)/2$. Note that $a<\nu(2)/2$, and $b<\nu(2)$. Let A^* be the Hopf algebra order in kG^* generated by $\mathfrak{P}^{-a}(\chi-1)$ and $\mathfrak{P}^{-b}(\chi^2-1)$. Then, $\bar{k}\otimes_R A^*=\bar{k}[X,Y]/(X^2,Y^2)$, so that $\bar{k}\otimes_R A$ is primitively generated. We will see in Section 4 that $A\neq\mathbf{A}(\xi)$ for any group valuation ξ.

In the case where R is a principal ideal domain and ξ is a p-adic order-bounded group valuation, we can refine the construction used in the proof of Proposition 3.2 to get a basis for $A=\mathbf{A}(\xi)$ as a R-module. Let $(\mathscr{B},\rho)$ be a complete p-adic weighted filtration trivially extending $\mathbf{F}(\xi)$. We can find a sequence of elements $g_1,\ldots,g_k$ such that if $N_0=\{1\}$ and $N_i=\langle g_1,\ldots,g_i\rangle$, then $\mathscr{B}=\{N_i\}$. Note that each $g_i{}^p\in N_{i-1}$ and that $N_k=G_+$. Let $h_1,\ldots,h_l$ be a set of representatives of the cosets of G_+ in G. Let π be a generator of the prime ideal P corresponding to the valuation ν and define the integer n_i by $n_i=\xi(g_i)/\nu(\pi)$. Let $u_i=\pi^{-n_i}(g_i-1)$.

Proposition 3.10. *If the ring of algebraic integers R is a principal ideal domain and if ξ is a p-adic order-bounded group valuation, then the set*

$$\{u_1^{e_1}\cdots u_k^{e_k}h_i \mid 0\leqslant e_r\leqslant p-1,\ 1\leqslant i\leqslant l\},$$

where u_r and h_i are as defined above, is a basis for $\mathbf{A}(\xi)$ over R.

Proof. By Corollary 3.8, it is sufficient to show that $\{u_1^{e_1} \cdots u_k^{e_k} \mid 0 \leqslant e_r \leqslant p-1\}$ is a basis for $A_+ = A \cap kG_+$. Because $\dim_R A_+ = |G_+| = p^k = |\{u_1^{e_1} \cdots u_k^{e_k}\}|$, it is sufficient to show that $\{u_1^{e_1} \cdots u_k^{e_k} \mid 0 \leqslant e_r \leqslant p-1\}$ spans A_+.

We will show by induction on i that monomials of the form $u_1^{e_1} \cdots u_i^{e_i}$, $0 \leqslant e_r \leqslant p-1$, span $A_i = A \cap kN_i$. This is clear for $i = 0$. Suppose it is true for $i-1$. Let $x = \xi(g_i)/\nu(\pi)$. Note that $\xi(ng_i^f)/\nu(\pi) = x$ for all $n \in N_{i-1}$, $1 \leqslant f \leqslant p-1$. Then A_i is spanned by monomials in A_{i-1} of the indicated form together with monomials of the form

$$u_i^{e_1} \cdots u_{i-1}^{e_{i-1}} \pi^{-x}(n_1 g_i^{f_1} - 1) \cdots \pi^{-x}(n_t g_i^{f_t} - 1),$$

where $0 \leqslant e_r \leqslant p-1$, $n_s \in N_{i-1}$, $1 \leqslant f_s \leqslant p-1$. Since $(ng_i^f - 1) = n(g_i^f - 1) + (n-1)$, for $n \in N_{i-1}$, $1 \leqslant f \leqslant p-1$, and since $(g_i^f - 1)n = n'(g_i^f - 1) + n' - n$, where $n' = g_i^f n g_i^{-f}$ is in N_{i-1}, it follows that A_i is spanned by monomials in A_{i-1} of the indicated form together with monomials of the form

$$u_1^{e_1} \cdots u_{i-1}^{e_{i-1}} \pi^{-x}(g_i^{f_i} - 1) \cdots \pi^{-x}(g_i^{f_t} - 1).$$

Since

$$g_i^f = ((g_i - 1) + 1)^f = \sum_{m=0}^{f} C_{f,m}(g_i - 1)^m, \tag{3.11}$$

we have

$$\pi^{-x}(g_i^f - 1) = \sum_{m=1}^{f} \pi^{(m-1)x} C_{f,m} \pi^{-mx}(g_i - 1)^m.$$

Therefore, A_i is spanned by monomials of the form

$$u_1^{e_1} \cdots u_{i-1}^{e_{i-1}} \pi^{-rx}(g_i - 1)^r = u_1^{e_1} \cdots u_{i-1}^{e_{i-1}} u_i^{r}, \tag{3.12}$$

for $0 \leqslant e_t \leqslant p-1$, $r \geqslant 0$. Since ξ is p-adic, $\xi(g_i^p) \geqslant p\xi(g_i)$ and it follows that $y = \xi(g_i^p)/\nu(\pi) \geqslant px$ and that $g_i^p \in N_{i-1}$. Therefore, using (3.11),

$$\begin{aligned} u_i^p &= \pi^{-px}(g_i - 1)^p \\ &= \pi^{y-px}\pi^{-y}(g_i^p - 1) + \sum_{m=1}^{p-1} \pi^{(m-p)x} C_{p,m} \pi^{-mx}(g_i - 1)^m \\ &= b + \sum_{m=1}^{p-1} \pi^{(m-p)x} C_{p,m} u_i^m, \end{aligned}$$

where $b \in A_{i-1}$. Since

$$\begin{aligned} \nu(\pi^{(m-p)x} C_{p,m}) &= (m-p)\, x\nu(\pi) + \nu(p) \\ &= (m-p)\, \xi(g_i) + \nu(p) \\ &\geqslant (m-p)\, \nu(p)/\varphi(\mathrm{order}(g_i)) + \nu(p) \\ &= ((m-p)/\varphi(p^a) + 1)\, \nu(p) \geqslant 0, \end{aligned}$$

where $\mathrm{order}(g_i) = p^a$, all the coefficients in the above sum are in R. Therefore, A_i is spanned by monomials of the form (3.12) with $r \leqslant p - 1$. This completes the proof of the proposition.

COROLLARY 3.13. *Let ξ be a p-adic order-bounded group valuation on the finite group G. Then, $\xi = \Xi\mathbf{A}(\xi)$.*

Proof. Since $\{u_1^{e_1} \cdots u_k^{e_k} h_i\}$ is a basis for $\mathbf{A}(\xi)$, so is $\{u_1^{e_1} \cdots u_k^{e_k}(h_i - 1)\}$. Let $\xi' = \Xi\mathbf{A}(\xi)$. By Corollary 3.3, $\xi' \geqslant \xi$. Suppose $\xi'(g) > \xi(g)$. If $\xi(g) = 0$, in the choice of coset representatives $h_1, \ldots, h_1$, choose g to represent its coset. If $\xi(g) > 0$, let i be the smallest integer such that $g \in N_i$. Choose g to be the element g_i that, together with N_{i-1}, generates N_i. In any case, $g - 1$ is a scalar multiple of a basis element of $\mathbf{A}(\xi)$. Say that $g - 1 = tw$, where $t \in R$, w is in the basis, and $\nu(t) = \xi(g)$. It is clear that in the definition of ξ', $I_g = t^{-1}R$, so $I_g^{-1} = tR$, so $\xi'(g) = \nu(t) = \xi(g)$, which gives a contradiction. This completes the proof of the corollary.

4. THE VALUE OF THE INTEGRAL

In this section, we compute the integral of a Hopf algebra order corresponding to a p-adic order-bounded group valuation. Let ν be a valuation, let p be the rational prime for which $\nu(p) \neq 0$, let G be a finite group, and let ξ be a p-adic order-bounded group valuation on G. Let $A = \mathbf{A}(\xi)$ and let L_A be the two-sided ideal of integrals in A. Since all of the elements of L_A are multiples of $\sum g$, to find L_A, it is sufficient to find $\epsilon(L_A)$. To find $\epsilon(L_A)$, it is sufficient to find $\nu(\epsilon(L_A))$. Recall that G_x denotes $\{g \mid \xi(g) \geqslant x\}$.

PROPOSITION 4.1. *Under the above hypothesis,*

$$\nu(\epsilon(L_A)) = \nu(|G|) - (p-1) \int_0^\infty \log_p(|G_x|)\, dx.$$

Since $\log_p(|G_x|) = 0$ *for sufficiently large x, the integral is meaningful.*

Note that if $x > 0$, then $|G_x|$ is a power of p, so that $\log_p(|G_x|)$ is an integer.

The proof of the proposition will be preceded by two lemmas.

LEMMA 4.2. *Assume that G is cyclic of order p, generated by g. Then,*

$$\nu(\epsilon(L_A)) = \nu(p) - (p-1)\,\xi(g).$$

Proof. Since each G_x is a subgroup of G and the only subgroups of G are $\{1\}$ and G, ξ is constant on $G - \{1\}$. Let $\xi(g) = r$ be this constant. Since

$$g^i = ((g-1)+1)^i = \sum_{j=0}^{i} C_{i,j}(g-1)^j,$$

it follows that

$$g^i - 1 = \sum_{j=1}^{i} C_{i,j}(g-1)^j, \qquad i < p.$$

Therefore,

$$\mathfrak{P}^{-r}(g^i - 1) = \sum_{j=1}^{i} \mathfrak{P}^{(j-1)r} C_{i,j}(\mathfrak{P}^{-r}(g-1))^j.$$

Therefore, A is generated by $\mathfrak{P}^{-r}(g-1)$.

Let P be the prime ideal in R corresponding to ν. Localizing at P, we may assume that R is a discrete valuation ring with maximal ideal $P = R\pi$. Note that $s = \xi(g)/\nu(\pi)$ is an integer; if $u = \pi^{-s}(g-1)$, then, $A = R[u]$. In particular, $1 = u^0, \ldots, u^{p-1}$ is a basis for A over R. Let Λ be a nonsingular left integral [9] in A. Since A is generated by u, and $\epsilon(u) = 0$, Λ can be characterized as follows: Every $x \in A$ such that $ux = 0$ is a multiple of Λ. Since

$$0 = g^p - 1 = \sum_{i=1}^{p} C_{p,i}(g-1)^i,$$

it follows that

$$\begin{aligned} 0 &= \sum_{i=1}^{p} C_{p,i}\pi^{si}(\pi^{-s}(g-1))^i \\ &= \sum_{i=1}^{p} \pi^{si} C_{p,i} u^i. \end{aligned}$$

Therefore,

$$u^p = -\sum_{i=1}^{p-1} \pi^{-s(p-i)} C_{p,i} u^i.$$

Since ξ is order bounded, $\xi(g) \leqslant \nu(p)/(p-1)$, so $s(p-1)\,\nu(\pi) \leqslant \nu(p)$. This implies that $s(p-i)\,\nu(\pi) \leqslant \nu(p)$. Therefore, since p divides $C_{p,i}$, the coefficients used to express u^p as a linear combination of $u,\ldots, u^{p-1}$ are all in R. If $x = \sum_{i=0}^{p-1} a_i u^i$ satisfies $ux = 0$, we have

$$\begin{aligned} 0 &= ux \\ &= \sum_{i=0}^{p-1} a_i u^{i+1} \\ &= \sum_{i=0}^{p-2} (a_i - \pi^{-s(p-i-1)} C_{p,i+1} a_{p-1})\, u^{i+1}. \end{aligned}$$

Therefore,

$$a_i = \pi^{-s(p-i-1)} C_{p,i+1} a_{p-1}\,,$$

for $i = 0,\ldots, p-2$. It is clear that we can describe A as follows: $A = \sum_{i=0}^{p-1} a_i u^i$, $a_{p-1} = e$ is a unit and the other a_i are given by the above equation. Therefore,

$$\begin{aligned} \nu(\epsilon(L_A)) &= \nu(\epsilon(A)) \\ &= \nu(a_0) \\ &= \nu(\pi^{-s(p-1)} C_{p,1}) \\ &= -s(p-1)\,\nu(\pi) + \nu(p) \\ &= \nu(p) - (p-1)\,\xi(g). \end{aligned}$$

Q.E.D.

LEMMA 4.3. *Assume $\xi(g) > 0$ for all $g \in G$. Let $A = \mathbf{A}(\xi)$. Let $(\mathscr{B}, \rho)$ be a complete trivial extension of $\mathbf{F}(\xi)$. Then*

$$\nu(\epsilon(L_A)) = \nu(|\, G \,|) - (p-1) \sum \rho(N),$$

where the sum is taken over all $N \neq \{1\}$ in $\mathscr{B}$.

Proof. Since $\xi(g) > 0$ for all g in G, $|\, G \,| = p^n$. We prove the lemma by induction on n. For $n = 1$, the lemma reduces to Lemma 4.2. For $n > 1$, let G_1 be the group in $\mathscr{B}$ of index p in G, let $G_2 = G/G_1$, let A_1 be the Hopf algebra order in kG_1 given by $A_1 = \mathbf{A}(\xi \mid G_1)$ and let A_2 be the Hopf algebra order in kG_2 given by $A_2 = \mathbf{AX}((\mathscr{B}, \rho)/G_1)$. It follows from Corollary 3.13 that $A_1 = A \cap kG_1$. Also, the image of A in kG_2 under the map $kG_1 \to kG_2$ is exactly A_2. It follows from Proposition 2.1 that

$$\nu(\epsilon(L_A)) = \nu(\epsilon(L_{A_1})) + \nu(\epsilon(L_{A_2})).$$

By induction,

$$\nu(\epsilon(L_{A_1})) = \nu(|\, G_1 \,|) - (p-1) \sum{}' \rho(N), \tag{4.4}$$

where $\sum'$ is the sum over all $N \neq \{1\}$, G in $\mathscr{B}$. By Lemma 4.2, if the image of $g \in G$ generates G_2,

$$\begin{aligned} \nu(\epsilon(L_{A_2})) &= \nu(p) - (p-1)\,\xi(g) \\ &= \nu(|\,G_2\,|) - (p-1)\,\rho(G). \end{aligned} \tag{4.5}$$

Adding (4.4) and (4.5) to get $\nu(\epsilon(L_A))$ completes the proof of the lemma.

Proof of Proposition 4.1. By Corollary 3.13, $A_+ = A \cap kG_+ = \mathbf{A}(\xi \mid G_+)$. Also, the image of A in kG/G_+ is just RG/G_+ so

$$\nu(\epsilon(L_A)) = \nu(\epsilon(L_{A_+})) + \nu(\epsilon(L_{RG/G_+})).$$

Let $(\mathscr{B}, \rho)$ be a complete trivial extension of $\mathbf{F}(\xi)$. If $G_+ \subset G$, extend $(\mathscr{B}, \rho)$ by adding G to the set $\mathscr{B}$, and defining $\rho(G) = 0$. By Lemma 4.3,

$$\nu(\epsilon(L_{A_+})) = \nu(|\,G_+\,|) - (p-1) \textstyle\sum \rho(N),$$

where the sum is taken over all subgroups $N \neq G$ in $\mathscr{B}$. Note that

$$\nu(\epsilon(L_{RG/G_+})) = \nu(|\,G/G_+\,|).$$

Therefore,

$$\begin{aligned} \nu(\epsilon(L_A)) &= \nu(|\,G_+\,|) - (p-1) \textstyle\sum \rho(N) + \nu(|\,G/G_+\,|) \\ &= \nu(|\,G\,|) - (p-1) \textstyle\sum \rho(N). \end{aligned}$$

Let $0 = x_0 < x_1 < \cdots < x_k$ be the distinct finite values of ρ, let $n_i = |\{N \in \mathscr{B} \mid \rho(N) = x_i\}|$, and let

$$s_i = n_i + \cdots + n_k = \log_p(|\,G_{x_i}\,|).$$

Then,

$$\begin{aligned} \textstyle\sum \rho(N) &= \sum_{i=1}^{k} x_i n_i \\ &= \sum_{i=1}^{k} (x_i - x_{i-1})\, s_i \\ &= \sum_{i=1}^{k} (x_i - x_{i-1}) \log_p(|\,G_{x_i}\,|) \\ &= \int_0^\infty \log_p(|\,G_x\,|)\, dx. \end{aligned}$$

The proposition follows.

If Z_{p^n} is a cyclic group of order p^n, it is easily checked that

$$\begin{aligned} \xi_0(g) &= \nu(p)/\varphi(\text{order}(g)), \qquad && \text{if} \quad g \neq 1 \\ &= \infty, && \text{if} \quad g = 1, \end{aligned}$$

is a p-adic order-bounded group valuation on Z_{p^n}. Clearly, it is the unique maximal order-bounded group valuation on this group.

COROLLARY 4.6. *If ξ is an order-bounded group valuation on Z_{p^n} and if $A = \mathbf{A}(\xi)$, then*

$$\nu(\epsilon(L_A)) \geqslant \nu(p)(n - (p^n - 1)/(p^n - p^{n-1})).$$

Proof. Let $A_0 = \mathbf{A}(\xi_0)$, where ξ_0 is the maximal order-bounded group valuation defined above. Since $\xi \leqslant \xi_0$, $A \subseteq A_0$, so $L_A \subseteq L_{A_0}$. Therefore $\nu(\epsilon(L_A)) \geqslant \nu(\epsilon(L_{A_0}))$. By Lemma 4.3,

$$\begin{aligned} \nu(\epsilon(L_{A_0})) &= \nu(p^n) - (p - 1) \sum_{i=1}^{n} \nu(p)/\varphi(p^i) \\ &= n\nu(p) - \nu(p) \sum_{i=1}^{n} 1/p^{i-1} \\ &= \nu(p)\,(n - (p^n - 1)/(p^n - p^{n-1})). \end{aligned}$$

This completes the proof of the corollary.

We now show that the order A constructed in Example 3.9 is not equal to $\mathbf{A}(\xi)$ for any ξ. Note that $A^* = \mathbf{A}(\xi^*)$, where $\xi^*(\chi) = \xi^*(\chi^3) = a$ and that $\xi^*(\chi^2) = b$. The conditions on a, b given in Example 3.9 imply that ξ^* is a p-adic order-bounded group valuation. By Proposition 4.1,

$$\begin{aligned} \nu(\epsilon(L_{A^*})) &= \nu(4) - (2a + (b - a)), \\ &= \nu(4) - (a + b). \end{aligned}$$

By [8, Proposition 2.2],

$$\nu(\epsilon(L_A)) = \nu(4) - \nu(\epsilon(L_{A^*})) = a + b.$$

If $A = \mathbf{A}(\xi)$ for some ξ, by Corollary 4.4,

$$\begin{aligned} \nu(\epsilon(L_A)) &\geqslant \nu(2)(2 - (4 - 1)/(4 - 2)), \\ &= \nu(2)/2. \end{aligned}$$

But a and b were chosen so that $a + b < \nu(2)/2$. Therefore, $A \neq \mathbf{A}(\xi)$.

5. Degrees of Irreducible Representations

In this section, we apply Proposition 4.1 of this paper and [8, Proposition 4.2] to get a new bound on the degrees of the absolutely irreducible representations of a finite group.

Theorem 5.1. *Let p be a fixed rational prime, let G be a finite group, and let ξ be a group valuation on G such that $\xi(g) > 0$ implies that* order(g) *is a power of p. Let*

$$K = \max_{g \neq 1}\{\xi(g)\,\varphi(\text{order}(g))\},$$

where φ is the Euler totient function. If V is an absolutely irreducible representation of G, then, for any valuation ν on k,

$$\nu(\dim_k V) \leqslant \nu(|\,G\,|) - \nu(p)\,((p-1)/K)\int_0^\infty \log_p(|\,G_x\,|)\,dx,$$

where $G_x = \{g \in G \mid \xi(g) \geqslant x\}$.

Proof. If $\nu(p) = 0$, then the theorem is just a restatement of the Frobenius theorem. Therefore, we may assume that $\nu(p) \neq 0$. Let ν' be the valuation $(K/\nu(p))\nu$. Note that $\nu'(p) = K$.

First, we consider the case where all the values of ξ are rational multiples of K. Let d the least common multiple of the denominators of these rational multiples. Replacing k by a finite extension on which there is a valuation (which we will also call ν') extending ν' whose ramification index over ν' is a multiple of d, we may assume that the range of ξ is contained in the range of ν'. Since

$$\xi(g)\,\varphi(\text{order}(g)) \leqslant K = \nu'(p),$$

the group valuation ξ is order bounded with respect to the valuation ν'. Let $A = \mathbf{A}(\xi)$ and $\xi' = \Xi(A)$. Since ξ' is p-adic and $A = \mathbf{A}(\xi')$.

$$\nu'(\epsilon(L_A)) = \nu'(|\,G\,|) - (p-1)\int_0^\infty \log_p(|\,G_x'\,|)\,dx,$$

where $G_x' = \{g \in G \mid \xi'(g) \geqslant x\}$. Since $\xi \leqslant \xi'$, we have that $G_x \subseteq G_x'$, so that $\log_p(|\,G_x\,|) \leqslant \log_p(|\,G_x'\,|)$. Therefore,

$$\nu'(\epsilon(L_A)) \leqslant \nu'(|\,G\,|) - (p-1)\int_0^\infty \log_p(|\,G_x\,|)\,dx.$$

By [8, Proposition 4.2], $\nu'(\dim_k V) \leqslant \nu'(\epsilon(L_A))$. Therefore,

$$\nu'(\dim_k V) \leqslant \nu'(|\,G\,|) - (p-1)\int_0^\infty \log_p(|\,G_x\,|)\,dx.$$

Multiplying this inequality by $\nu(p)/K$, we get the inequality in the statement of the theorem.

Before we prove the general case of the theorem, we will prove the following lemma:

LEMMA 5.2. *Let $S \subseteq \mathbf{R}^n$ be the set of solutions of the system of inequalities*

$$p_i \leqslant X_i \leqslant q_i, \qquad \text{where} \quad p_i, q_i \in \mathbf{Q}, \tag{5.3}$$

$$X_k \geqslant \min\{X_i, X_j\}, \qquad \text{for} \quad (i, j, k) \in I, \tag{5.4}$$

and

$$X_k \geqslant r_{ki}X_i + s_{kj}X_j, \qquad \text{for } (i, j, k) \in J, \text{ where } r_{ki}, s_{kj} \in \mathbf{Q}. \tag{5.5}$$

Then, for every $\mathbf{x} \in S$, there exist $\mathbf{y} \in S \cap \mathbf{Q}^n$ arbitrarily close to $\mathbf{x}$.

Proof. Fix $\mathbf{x} = (x_i) \in S$ and consider the following system of equations:

$$\begin{aligned}
&\text{if } x_i = a_i \text{ is rational}, \qquad X_i = a_i;\\
&\text{if } x_i = x_j, \qquad X_i - X_j = 0;\\
&\text{if } r_{ki}x_i + s_{kj}x_j = x_k, \qquad r_{ki}X_i + s_{kj}X_j - X_k = 0.
\end{aligned}$$

We have a system of linear equations with rational coefficients that has a solution (x_i). Therefore, we can find indices $i_1, \ldots, i_k$ such that this system is equivalent to a system

$$X_j = \sum_{l=1}^{k} a_{jl}X_{i_l} + b_j,$$

where the a_{jl} and the b_j are rational and such that any assignment of values $X_{i_1} = c_{i_1}, \ldots, X_{i_k} = c_{i_k}$ gives a solution to the system. Pick $c_{i_l}^{(r)} \in \mathbf{Q}$ converging to x_{i_l} and define

$$c_j^{(r)} = \sum_{l=1}^{k} a_{jl}c_{i_l}^{(r)} + b_j.$$

Then, $\mathbf{c}^{(r)} = (c_j^{(r)})$ converges to $\mathbf{x}$. We claim that for r sufficiently large, $\mathbf{c}^{(r)} \in S$.

First, $\mathbf{c}^{(r)}$ satisfies (5.3) for r sufficiently large: Suppose $p_i \leqslant x_i \leqslant q_i$. If x_i is rational, then $c^{(r)} = x_i$. Otherwise $p_i < x_i < q_i$, so for r sufficiently large, $p_i \leqslant c_i^{(r)} \leqslant q_i$. Now, we consider (5.4): If $x_i \leqslant x_j$, then $c_i^{(r)} \leqslant c_j^{(r)}$ for r sufficiently large, for, either $x_i = x_j$, which implies that $c_i^{(r)} = c_j^{(r)}$, or $x_i < x_j$, which, together with the facts that $c_i^{(r)}$ converges to x_i and $c_j^{(r)}$ converges to x_j, implies that $c_i^{(r)} \leqslant c_j^{(r)}$ for r sufficiently large. Since

$$\begin{aligned}
\min\{x_i, x_j\} &= x_i, \qquad \text{if} \quad x_i \leqslant x_j,\\
&= x_j, \qquad \text{otherwise.}
\end{aligned}$$

It is clear that if

$$\min\{x_i, x_j\} \leqslant x_k,$$

then

$$\min\{c_i^{(r)}, c_j^{(r)}\} \leqslant c_k^{(r)}$$

for r sufficiently large. Therefore, $\mathbf{c}^{(r)}$ satisfies (5.4) for r sufficiently large.

Suppose that $x_k \geqslant r_{ki}x_i + s_{kj}x_j$. Then, either $r_{ki}x_i + s_{kj}x_j = x_k$, so that $r_{ki}c_i^{(r)} + s_{kj}c_j^{(r)} = c_k^{(r)}$, or $r_{ki}x_i + s_{kj}x_j < x_k$, so that, for r sufficiently large, $r_{ki}c_i^{(r)} + s_{kj}c_j^{(r)} \leqslant c_k^{(r)}$. Therefore, $\mathbf{c}^{(r)}$ satisfies (5.5) for r sufficiently large. This completes the proof of the lemma.

We now return to the proof of Theorem 5.1.

Enumerate the nonidentity elements of the group $g_1, ..., g_n$, and let $x_i = \xi(g_i)/K$. Then, (x_i) satisfies the system of inequalities:

$$\begin{aligned} 0 \leqslant X_i &\leqslant 1/\varphi(\mathrm{order}(g_i)) && \text{if} \quad \mathrm{order}(g_i) = p^s, \\ &= 0, && \text{otherwise;} \end{aligned} \tag{5.6}$$

$$X_k \geqslant \min\{X_i, X_j\}, \qquad \text{if} \qquad g_i g_j = g_k, \tag{5.7}$$

$$X_k \geqslant X_i + X_j, \qquad \text{if} \qquad [g_i, g_j] = g_k. \tag{5.8}$$

By Lemma 5.2, for each $\epsilon > 0$ there exists $(y_i) \in \mathbf{Q}^n$ with $|x_i - y_i| < \epsilon$ and with (y_i) satisfying the same relations (5.6)–(5.8). Let $\eta(g_i) = Ky_i$, and let $\eta(1) = \infty$. Then, η is a group valuation that satisfies the hypothesis of the theorem. Since all of the nonzero finite values of η are rational multiples of each other, they are all rational multiples of $\max\{\eta(g)\,\varphi(\mathrm{order}(g)) \mid g \neq 1\}$. Applying the first part of the proof of the theorem to η, we conclude that

$$\nu(\dim_k V) \leqslant \nu(|G|) - \nu(p)\,((p-1)/L) \int_0^\infty \log_p(|H_x|)\,dx, \tag{5.9}$$

where

$$L = \max_{g \neq 1}\{\eta(g)\,\varphi(\mathrm{order}(g))\}$$

and

$$H_x = \{g \in G \mid \eta(g) \geqslant x\}.$$

Note that

$$|\eta(g) - \xi(g)| < K\epsilon$$

and that

$$H_{x+K\epsilon} \subseteq G_x \subseteq H_{x-K\epsilon}.$$

Therefore,

$$|L - K| < \varphi(|G|)\,K\epsilon$$

and

$$\left| \int_0^\infty \log_p(|H_x|)\,dx - \int_0^\infty \log_p(|G_x|)\,dx \right| < \log_p(|G|)\,K\epsilon.$$

Therefore, by taking ϵ sufficiently small, the right-hand side of (5.9) can be made arbitrarily close to

$$\nu(|G|) - \nu(p)\,((p-1)/K) \int_0^\infty \log_p(|G_x|)\,dx.$$

The theorem follows.

6. A Computation

One obvious question is: How does the bound for degrees of absolutely irreducible representations of a finite group that is given in Theorem 5.1 compare with the bound given by Ito's theorem? In some cases, such as when G is cyclic of order p^n with n large, the bound given by Theorem 5.1 is much worse than that given by Ito's theorem. In this section, we compare the bounds given by Theorem 5.1 and Ito's theorem for the groups of order 2^n, $n \leqslant 6$, described in [3]. We will see that for these groups, in those cases where Ito's theorem does not give the best possible bound, Theorem 5.1 gives a better bound.

Of the 341 groups of order 2^n, $0 \leqslant n \leqslant 6$, listed in [3], 30 are abelian, 165 are nonabelian and have a normal abelian subgroup of index 2, and 136 have an absolutely irreducible representation of degree 4 and a normal abelian subgroup of index 4. The remaining 10 are the only ones in which the bound given by Ito's theorem does not equal the maximal degree of the absolutely irreducible representations. All of these are in the family Γ_9 and have order 64. They have no absolutely irreducible representation of degree greater than 2 and all of the normal abelian subgroups have index not less than 4. In all of the groups of order 64 in the family Γ_9, $[G, G] = \mathscr{Z}(G)$ is an elementary abelian 2-group. Also $G/\mathscr{Z}(G)$ is an elementary abelian 2-group, so that all of the elements of G have order dividing 4. Define $\xi\colon G \to \mathbf{R} \cup \{\infty\}$ by

$$\begin{aligned} \xi(g) &= \tfrac{1}{2}, && \text{if } g \in G - [G, G], \\ &= 1, && \text{if } g \in [G, G] - \{1\}, \\ &= \infty, && g = 1. \end{aligned}$$

We now show that ξ is a group valuation: Condition (1) of Definition 1.1 is obviously satisfied. We now consider (2). Note that $\xi(gh) \geqslant \frac{1}{2}$ always.

Suppose that $\min\{\xi(g), \xi(h)\} = 1$. Then, $g, h \in \mathscr{Z}(G)$ so that $gh \in \mathscr{Z}(G)$, so $\xi(gh) \geqslant 1$. If $\min\{\xi(g), \xi(h)\} = \infty$, then $g = h = 1$, so that $gh = 1$, so $\xi(gh) = \infty$. Therefore, condition (2) is satisfied. We now consider condition (3). If $\xi(g) = \xi(h) = \frac{1}{2}$, since $[g, h] \in [G, G]$,

$$\xi([g, h]) \geqslant 1 = \xi(g) + \xi(h).$$

If $\xi(g)$ or $\xi(h) > \frac{1}{2}$, then g or h is in $\mathscr{Z}(G)$, so that $[g, h] = 1$, so $\xi([g, h]) = \infty \geqslant \xi(g) + \xi(h)$. Therefore, condition (3) is satisfied and ξ is a group valuation. Applying Theorem 5.1,

$$K = \max_{g \neq 1}\{\xi(g)\, \varphi(\mathrm{order}(g))\} = 1$$

and

$$\int_0^\infty \log_2(|\, G_x \,|)\, dx = \int_0^{1/2} 6dx + \int_{1/2}^1 3dx = \tfrac{9}{2}\,,$$

so for any absolutely irreducible representation V

$$\nu(\dim_k V) \leqslant \nu(2^6) - \nu(2)9/2 = 3\nu(2)/2.$$

In other words,

$$\log_2(\dim_k V) \leqslant 3/2.$$

Of course, since $\log_2(\dim_k V)$ must be an integer, we have that $\dim_k V$ must divide 2, so that Theorem 5.1 gives the correct bound for the stem groups of the family Γ_9.

7. Global Considerations and Questions

Thus far, we have considered only group valuations associated with a fixed valuation. In this section, we describe global group valuations and indicate their relation to orders in kG. Denote by $\mathscr{I}$ the group of fractional ideals in k. Let ψ be the function defined by

$$\begin{aligned} \psi(n) &= p, \qquad \text{if} \quad n = p^s, \\ &= 1, \qquad \text{otherwise.} \end{aligned}$$

Note that $\psi(n) = \exp \Lambda(n)$, where the negative of the logarithmic derivative of the zeta function is the generating function of $\Lambda(n)$ [4]. Recall that φ is the Euler totient function.

DEFINITION 7.1. Let G be a finite group. A *global group valuation* is a function $\zeta\colon G \to \mathscr{I} \cup \{\{0\}\}$ satisfying:

(1) $\zeta(g) \subseteq R$; $\zeta(g) = \{0\}$, if and only if $g = 1$,

(2) $\zeta(gh) \subseteq \zeta(g) + \zeta(h)$,

(3) $\zeta([g, h]) \subseteq \zeta(g)\,\zeta(h)$.

If

$$\zeta(g)^{\varphi(\operatorname{order}(g))} \supseteq \psi(\operatorname{order}(g))\,R$$

for all $g \neq 1$ in G, then ζ is said to be *order bounded.* The order-bounded global valuation ζ is called *p-adic* if

$$\zeta(g^{\psi(\operatorname{order}(g))}) \subseteq \zeta(g)^{\psi(\operatorname{order}(g))}$$

for all $g \neq 1$ in G.

Note that if ζ is an order-bounded global group valuation and if $g \neq 1$, then all prime divisors of $\zeta(g)$ must also divide $|G|$. Let $\nu_1, \dots, \nu_k$ be a set of representatives of the equivalence classes of valuations ν for which $\nu(|G|) \neq 0$ and let $\mathfrak{P}_i^x$ be the fractional ideal for which

$$\nu_i(\mathfrak{P}_i^x) = x, \qquad \nu(\mathfrak{P}_i^x) = 0,$$

if ν is not equivalent to ν_i.

PROPOSITION 7.2. *Let G be a finite group and let $\nu_1, \dots, \nu_k$ be as above. Then, there is a one–one correspondence between order-bounded global group valuations ζ and k-tuples $(\xi_1, \dots, \xi_k)$ of group valuations such that ξ_i is order bounded with respect to ν_i. The correspondence is given by $\zeta \mapsto (\xi_1, \dots, \xi_k)$, where*

$$\xi_i(g) = \nu_i(\zeta(g)),$$

and $(\xi_1, \dots, \xi_k) \mapsto \zeta$, where

$$\begin{aligned} \zeta(g) &= \prod \mathfrak{P}_i^{\xi_i(g)}, && \text{if} \quad g \neq 1, \\ &= \{0\}, && \text{if} \quad g = 1. \end{aligned}$$

Under this correspondence, p-adic global group valuations correspond to k-tuples of p-adic group valuations.

Proof. Let ζ be an order-bounded global group valuation. It is immediate that $\xi_i = \nu_i \circ \zeta$ is a group valuation: conditions (1)–(3) of Definition 7.1 imply the corresponding conditions of Definition 1.1 for ξ_i. We now show that ξ_i is order bounded. Observe that

$$\nu_i(\zeta(g)^{\varphi(\operatorname{order}(g))}) \leqslant \nu_i(\psi(\operatorname{order}(g)).$$

This implies that

$$\xi_i(g) = \nu_i(\zeta(g)) \leqslant \nu_i(\psi(\mathrm{order}(g)))/\varphi(\mathrm{order}(g)).$$

If order(g) is not a prime power, $\psi(\mathrm{order}(g)) = 1$, so $\xi_i(g) \leqslant 0$. Since $\xi_i(g) \geqslant 0$, we have that $\xi_i(g) = 0$ in this case. Otherwise, $\psi(\mathrm{order}(g)) = q$, where order$(g) = q^s$, and

$$\xi_i(g) \leqslant \nu_i(q)/\varphi(\mathrm{order}(g)).$$

Therefore, ξ_i is an order-bounded group valuation.

Now, let $(\xi_1, \ldots, \xi_k)$ be a k-tuple of order-bounded group valuations. It is immediate that ζ is a global group valuation: conditions (1)–(3) of Definition 1.1 imply the corresponding conditions of Definition 7.1. Also, a computation analogous to the one given in the above paragraph shows that ζ is order bounded.

We now show that ζ is p-adic if and only if each ξ_i is p-adic. Let $g \neq 1$ be an element of G. If order(g) is not a prime power, then $\zeta(g) = R$ and $\xi_i(g) = 0$ for all i, since ζ and the ξ_i are order bounded. Therefore, in this case it is trivial that

$$\zeta(g^{\psi(\mathrm{order}(g))}) \subseteq \zeta(g)^{\psi(\mathrm{order}(g))}$$

and that

$$\xi_i(g^{p_i}) \geqslant p_i \xi_i(g),$$

where p_i is the rational prime such that $\nu_i(p_i) \neq 0$. Suppose now that order$(g) = p^s$. If ζ is p-adic, then,

$$\zeta(g^p) \subseteq \zeta(g)^p,$$

so

$$\xi_i(g^p) \geqslant p\xi_i(g).$$

If $p = p_i$, this says that ξ_i is p-adic. If $p \neq p_i$, then $\xi_i(g) \leqslant \nu_i(p)/\varphi(\mathrm{order}(g))$, so that $\xi_i(g) = 0$ and again, $\xi_i(g^{p_i}) \geqslant p_i\xi_i(g)$. Now, suppose that each ξ_i is p-adic. Using an argument analogous to the one just given, $\xi_i(g^p) \geqslant p\xi_i(g)$, either because $p = p_i$ and ξ_i is p-adic, or because $p \neq p_i$ and so $\xi_i(g) = 0$. This implies that $\zeta(g^p) \subseteq \zeta(g)^p$, which says that

$$\zeta(g^{\psi(\mathrm{order}(g))}) \subseteq \zeta(g)^{\psi(\mathrm{order}(g))}.$$

Since the maps we have defined are clearly inverses of each other, the correspondence we have defined is a bijection. This completes the proof of the proposition.

The relation between global group valuations and Hopf algebra orders in kG can be described directly in a simple manner:

PROPOSITION 7.3. *Let G be a finite group. If A is a Hopf algebra order in kG, let*

$$I_g = \{x \in k \mid x(g-1) \in A\}.$$

Then,

$$\begin{aligned} \zeta(g) &= \{0\}, && \text{if} \quad g = 1, \\ &= I_g^{-1}, && \text{if} \quad g \neq 1, \end{aligned}$$

is a p-adic order-bounded global group valuation. If ζ is an order-bounded global group valuation, then

$$R[\zeta(g)^{-1}(g-1)],$$

where g ranges over the nonidentity elements of G, is a Hopf algebra order in kG.

Proof. Let A be a Hopf algebra order in kG. By Proposition 3.1, $\xi_i(g) = v_i(\zeta(g))$ is a p-adic order-bounded group valuation. Therefore, ζ is a p-adic order-bounded global group valuation by Proposition 7.2.

Now, suppose that ζ is an order-bounded global group valuation corresponding to $(\xi_1, \ldots, \xi_k)$. Let $A = R[\zeta(g)^{-1}(g-1)]$ and let $A_i = R[\mathfrak{P}_i^{-\xi_i(g)}(g-1)]$. Then, each A_i is a Hopf algebra order in kG by Proposition 3.2. Since $A_i \subseteq A$, we have that $A_1 \cdots A_k \subseteq A$. Localizing at each prime, we have equality so that $A_1 \cdots A_k = A$. But $A_1 \cdots A_k$ is clearly a finitely generated R-coalgebra and A is clearly a R-algebra. This shows that it is a Hopf algebra order. This completes the proof of the proposition.

It follows from Corollary 3.13 that Proposition 7.3 gives a bijection between the set of p-adic order-bounded global group valuations on G and certain Hopf algebra orders in kG. It is not known how to characterize those Hopf algebra orders that arise from global group valuations.

In [8], a method of constructing nontrivial Hopf algebra orders in kG was given that gives Ito's bound on the degrees of absolutely irreducible representations. In this paper, we have given another method of constructing orders that gives a bound on the degrees of absolutely irreducible representations. What other methods of constructing orders can be found? Is it possible to find a reasonably effective method of constructing orders that will give a bound that includes both Ito's theorem and Theorem 5.1? For definiteness, let us say that the bound should be computable in terms of the lattice of normal subgroups of G together with certain additional information, such as commutator relations between normal subgroups and their exponents.

Related to this is the question of how large an order can actually exist in kG. We conjecture that if G is a finite nilpotent group, and if d is the least common multiple of the degrees of the irreducible representations of G over $\mathbf{C}$, then there exists a Hopf algebra order A in kG with $\epsilon(L_A) = dR$.

Very little seems to be known about classifying orders in kG. One possible approach is to determine all possible orders in group algebras of cyclic groups and then to study the embedding of the cyclic groups in the group. The orders in the group algebra of a group of order p were first classified in [17]; the orders in a cyclic group of order p^2 do not seem to be known. Another approach to this classification problem is to use an arithmetical analog of the divided power techniques used in studying the structure of pointed irreducible cocommutative Hopf algebras in positive characteristic. From this point of view, the results of this paper classify orders that are of coheight 0.

Acknowledgments

I wish to thank the Mathematics Department of Rutgers University for their hospitality during my sabbatical leave. Computing services used in this research were provided by the Center for Computer and Information Services of Rutgers University. Their assistance is gratefully acknowledged.

References

1. V. K. A. M. Gugenheim, On extensions of algebras, co-algebras, and Hopf algebras. I, *Amer. J. Math.* **84** (1962), 349–382.
2. V. K. A. M. Gugenheim, Cohomology theory in the category of Hopf algebras, *in* "Colloque de Topologie," pp. 137–148. Brussels, 1964, Librairie Universitaire, Louvain, 1966.
3. M. Hall Jr. and J. K. Senior, "The Groups of Order $2^n (n \leqslant 6)$," MacMillan, New York, 1964.
4. G. H. Hardy and E. M. Wright, "An Introduction to the Theory of Numbers," Clarendon Press, Oxford, 1954.
5. R. G. Larson, Group rings over Dedekind domains. I, *J. Algebra* **5** (1967), 358–361.
6. R. G. Larson, Group rings over Dedekind domains. II, *J. Algebra* **7** (1967), 278–279.
7. R. G. Larson, Characters of Hopf algebras, *J. Algebra* **17** (1971), 352–368.
8. R. G. Larson, Orders in Hopf algebras, *J. Algebra* **22** (1972), 201–210.
9. R. G. Larson and M. E. Sweedler, An associative orthogonal bilinear form for Hopf algebras, *Amer. J. Math.* **91** (1969), 75–94.
10. K. Newman, A correspondence between bi-ideals and sub-Hopf algebras in cocommutative Hopf algebras, *J. Algebra* **36** (1975), 1–15.
11. U. Oberst and H.-J. Schneider, Über Untergruppen endlicher algebraischer Gruppen, *Manuscripta Math.* **8** (1973), 217–241.
12. U. Oberst, Untergruppen formeller Gruppen von endlichen index, *J. Algebra* **31** (1974), 10–44.
13. C. Schoeller, Étude de la Catégorie des algèbres de Hopf commutatives connexes sur un corps, *Manuscripta Math.* **3** (1970), 133–155.

14. W. M. SINGER, Extension theory for connected Hopf algebras, *J. Algebra* **21** (1972), 1–16.
15. M. E. SWEEDLER, "Hopf Algebras," Benjamin, New York, 1969.
16. M. TAKEUCHI, A correspondence between Hopf ideals and sub-Hopf algebras, *Manuscripta Math.* **7** (1972), 251–270.
17. J. TATE AND F. OORT, Group schemes of prime order, *Ann. Sci. École Norm. Sup.* (4) **3** (1970), 1–21.
18. E. WEISS, "Algebraic Number Theory," McGraw–Hill, New York, 1963.
19. G. C. WRAITH, Abelian Hopf algebras, *J. Algebra* **6** (1967), 135–156.
20. H. ZASSENHAUS, On group valuations.